FGP – FACULDADE GENNARI & PEARTREE
Sistemas de Informação

GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Alex de Oliveira Barros Maior
Fábio Antonio dos Santos
Sabrina Cristiane Dal Lacqua

PEDERNEIRAS – SP
2006

FGP – FACULDADE GENNARI & PEARTREE
Sistemas de Informação

GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Alex de Oliveira Barros Maior
Fábio Antonio dos Santos
Sabrina Cristiane Dal Lacqua

Trabalho apresentado como requisito obrigatório à conclusão do Curso de Bacharelado de Sistema de Informação da Faculdade Gennari & Peartree.

Orientador: César Sant'Anna Junior

PEDERNEIRAS – SP
2006

Dedicamos este trabalho a nossos pais, pelo admirável apoio e incentivo.

Agradecimentos

À Deus, aos nossos familiares, ao nosso orientador Cezar Sant'Anna Junior, a todos os professores, a empresa SAF aos nossos amigos e a todos que de alguma forma contribuíram para o desenvolvimento deste trabalho.

“Sabedoria é a capacidade de prever as conseqüências a longo prazo das ações atuais, a disposição de sacrificar ganhos a curto prazo em favor de benefícios futuros e a habilidade de controlar o que é controlável e de não se afligir com o que não é. A essência da sabedoria, portanto, é a preocupação com o futuro. ”

ACKOFF, Planejamento Empresarial

RESUMO

A partir de definições de termos baseados na norma NBR ISO/IEC 17799:2001, e um estudo de caso em uma empresa, este trabalho busca favorecer o entendimento da Segurança da Informação, e também a conscientização da seriedade que se deve dar a ela principalmente nos dias atuais.

O trabalho mostrará que ao mesmo tempo em que no universo das informações os dados circulam na empresa com grande facilidade e muita rapidez, é importante não fechar os olhos para o perigo, ou seja, ele existe e não há como fugir das ameaças e dos riscos que a informação está sujeita constantemente.

Portanto, será fundamentada inclusive com dados estatísticos a importância de se adotar uma Política de Segurança da Informação nas empresas.

Palavras-chave: Segurança da Informação, Política da Segurança da Informação e NBR ISO/IEC 17799:2001.

ABSTRACT

From the definition of words based on the rule NBR ISO/IEC 17799:2001, and a company case study, this report searches to help the Information Security understanding, and also to get the conscience of the importance one should give to it specially in these days.

The report will show us that at the at same time, in the information universe, data go into companies in such an easy and fast way that is very important one not close its eyes to the danger, that means, the danger exists and one can not run away from the threat and the risks that the information is constantly under.

Therefore, the importance of having an Information Security Policy in the companies is founded including with statistic data.

Key-Word: Information Security, Information Security Policy and NBR/ISO/IEC 17799:2001

LISTA DE ILUSTRAÇÕES

Sumário

1 INTRODUÇÃO

O surgimento do computador fez com que a humanidade se sentisse diante de um novo desafio, ou seja, a habilidade para manuseá-lo. Hoje em dia ele se faz necessário nos lares, nas escolas, nas empresas e nos ambientes de lazer e a sua tecnologia nos serve de forma tão automática que muitas vezes passa despercebida.

Com a introdução da informática principalmente nas empresas, o trabalho foi agilizado e logo, os volumes de papéis, documentos circulados e arquivados foram consideravelmente reduzidos. A informação nos serve de forma automática, está embutida em todos os lugares e a cada dia que passa ela se torna cada vez mais acessível, por isso que se deve zelar por sua segurança.

Porém com todas essas inovações o principal combate das empresas é a garantia da segurança, ou seja, com tais mudanças fica cada vez mais difícil, tanto manter o sigilo das informações interna e externamente às empresas (o que se pode fazer para trancar um computador?), quanto preservar os dados para que não sejam perdidos (o que seria de um banco de dados se perdesse todos os dados de seus clientes?).

Afinal o que as empresas devem fazer para proteger suas informações? Que informações são essas? O que significa segurança da informação?

Na década de 60, surgiram os sistemas de computadores, com o propósito de substituir os sistemas manuais. A partir desse período a tecnologia, sobretudo na área de informática se torna cada dia mais influente no mundo dos negócios. Com o advento destes sistemas criados para ajudar as empresas a crescerem, prosperarem, capazes de trocar informações, controlar processos totalmente aliados a pesadas tecnologias e Internet as empresas necessitam de um cuidado cada vez maior com relação à segurança de informações.

Todas as respostas para essas questões podem ser encontradas ao longo dos seis capítulos em que está organizado este trabalho, os quais exploram questões e termos relacionados a Segurança da Informação. Ao mesmo tempo, um estudo de caso apresentando as principais falhas de segurança da informação na empresa analisada e em seguida a indicação de algumas soluções para os problemas descobertos.

O presente trabalho está organizado da seguinte forma. O capítulo um faz uma breve instrução do que será apresentado ao longo dos sete capítulos. O capítulo dois explana de forma clara o que significa a segurança da informação, enfocando na sua importância e nos seus benefícios de aplicação dentro das empresas. O capítulo três visa o esclarecimento de determinados componentes da Segurança da Informação, por exemplo, ativos, ameaças, vulnerabilidades e riscos. O capítulo quatro é um resumo da Norma *NBR ISO/IEC 17799/2001*, explicando todos os termos e componentes da mesma. No capítulo cinco é definido o que é uma Política de Segurança da Informação, evidenciando o seu papel fundamental dentro das empresas e o comprometimento de todos os envolvidos. No capítulo seis é desenvolvido um estudo de caso, o qual demonstrará a empresa questionada, a metodologia utilizada e as observações seguidas das soluções propostas pelo grupo com relação à segurança dentro da empresa. Por fim, o capítulo sete que contém a conclusão final do trabalho com o que foi absorvido e concluído pelo grupo.

2 O QUE É SEGURANÇA DA INFORMAÇÃO?

2.1 Informação: ativo de alta valorização

Laudon e Laudon (1999, p. 10, grifo nosso), tratando de informação menciona que:

> [...] vem da palavra Latina *informare*, que significa dar forma. A maioria dos filósofos acredita que é **a mente humana que dá forma aos dados** para criar uma "informação" e um conhecimento significativos. Platão e outros filósofos gregos tiraram esse conceito de um mundo de significado, intenção e conhecimento criado pelos seres humanos. Essas idéias estão no cerne da cultura ocidental.

A informação pode se manifestar de várias maneiras, isto é, de forma escrita, eletrônica ou impressa. Ela representa um conjunto de dados dos quais são modificados e tomam forma útil e significativa (LAUDON E LAUDON, 1999). E por isso, seja qual a forma de manifestação, a informação necessita estar sempre protegida.

De acordo com Sêmola (2003, p. 45), a informação pode ser definida como:

> Conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou máquinas em processos comunicativos (isto é, baseados em troca de mensagens) ou transacionais (isto é, processos em que sejam realizadas as operações que envolvam, por exemplo, a transferência de valores monetários).

Na sociedade do conhecimento, na qual vive-se, na qual as empresas estão sujeitas a várias mudanças a cada momento e precisa sempre estar se reciclando com relação às novidades do mundo dos negócios, a expressão "informação", que também pode ser definida como um ativo, tem um significado extremamente importante para a sua sobrevivência. Ela representa a porta para o crescimento e o sucesso.

Marcos Sêmola em sua obra "Gestão da Segurança da Informação"(2003, p.6), registrou que "O sangue da empresa é a informação". O autor faz uma analogia com a empresa e o corpo humano, da mesma maneira que os seres humanos dependem do sangue para a sobrevivência o mesmo acontece com a informação nas empresas. Assim como o sangue é circulado dos pés a cabeça, a informação é transportada incessantemente em todos os ambientes, é distribuída por todos os processos de negócio e responsável por manter a operação da empresa. Além disso, ela representa a inteligência competitiva dos negócios e é influenciada por fatores humanos, tecnológicos e físicos e por isso vive sob constante risco.

A informação segundo Ferreira e Araújo (2006) pode ser classificada segundo grau de importância em três grupos:

Informações Públicas: sua divulgação é livre. Não exige controle. Por exemplo: folhetos comerciais para o público em geral, ou dados divulgados pela imprensa e Internet.

Informações de Uso Interno: não devem ser expostas fora da empresa. Devem ser armazenadas em locais que não permitam o acesso público. Por exemplo: relatórios, pareceres, documentos e processos de negócio que interessam apenas aos funcionários da empresa.

Informações Confidenciais: exigem um cuidadoso esforço de proteção, uma vez que sua divulgação pode vir a causar prejuízos na empresa. Devem ser armazenadas em locais de máxima proteção, trancado e com acesso restrito. Quando elas estiverem contidas em meios eletrônicos, é imprescindível que sejam utilizados meios seguros para seu armazenamento, de preferência equipados com programas criptográficos e senhas de acesso. Por exemplo: contratos, senhas, balanços, dados cadastrais de clientes e funcionários e informações que devem ser protegidas por obrigatoriedade legal.

Independentemente da forma de como as informações são representadas, elas percorrem um ciclo de vida que pode ser definido por quatro fases. Essas fases segundo

(Sêmola, 2003) são: manuseio, armazenamento, transporte e descarte, que são descritas a seguir:

Manuseio: é a fase na qual a informação é originada e manejada, seja na digitação, folheamento de papéis, ou até mesmo na utilização de uma senha, por exemplo.

Armazenamento: é a continuidade da fase anterior, ou seja, depois de manipulada a informação deve seguir um caminho, por exemplo: gravação em uma mídia, preservação em um arquivo de ferro ou depósito em gaveta para eventos futuros.

Transporte: seguido do armazenamento esta fase representa o instante em que a informação é encaminhada, seja via e-mail, fax, ou mesmo uma informação confidencial que deve ser remetida pelo telefone.

Descarte: este é o momento do destino que a informação irá tomar, seja para a lixeira (material impresso), ou então um arquivo que vai ser excluído do computador, além de outros.

A seguir serão apresentados os conceitos sobre segurança.

2.2 Segurança: ação de prioridade

No sentido geral uma das definições encontradas no dicionário Aurélio, para o termo segurança é “[...] um estado e qualidade ou condição de seguro, assim também como convicção e certeza”. Dessa forma, a segurança de tempos em tempos passa a representar algo de fundamental precisão para tentar garantir que o negócio não esteja vulnerável, porém sempre disponível, ou ainda é mais do que isso, a segurança é uma obrigação. As soluções, as decisões e as saídas que hoje são seguras amanhã poderão não estar mais.

O termo segurança na visão da área de informática refere-se a todas as políticas, procedimentos e ferramentas técnicas utilizadas para defender sistemas de informação contra acessos e modificações não autorizados, alterações, destruições, roubo e danos físicos.

A segurança deve ser o primeiro passo a ser dado em uma empresa, e é exatamente por isso que o universo da tecnologia está sempre na busca por essa garantia. Essa busca deve ser diária, como pode ser visto a seguir.

2.3 Segurança da informação: cultivada dia-a-dia

Inicialmente deve-se ter conhecimento de que o enunciado "segurança da informação" pode exprimir dois sentidos, isto é, a segurança representada como um meio (instrumento) ou como um fim (conclusão). No primeiro ela propõe a garantia da proteção da informação, visando conformidades com as normas e dando continuidades aos processos de negócios na empresa. E no segundo representa quando a segurança é atingida por meio de práticas, políticas e processos que manipulam a informação.

Com a facilidade e a rapidez em que os dados circulam numa organização as informações podem ser usadas de forma nociva e se propagarem perigosamente. Portanto o perigo existe e não há como ignorar a necessidade de uma medida de segurança. Hoje em dia é preciso ter muita cautela.

Segurança da informação sempre é um assunto delicado dentro das corporações, tratado com reservas e até certo enigma. Muitas pessoas associam Segurança da Informação a uma mera aplicação de recursos tecnológicos, mas na verdade é um conjunto de procedimentos e controles no qual Tecnologia da Informação[1] certamente tem seu papel importante, todavia não é tudo.

Tecnologia da Informação[1]: engloba termos mais conhecidos no jargão brasileiro como informática, sistemas, telecomunicações, ciência da computação, processamento de dados, engenharia de sistemas e software.

De acordo com Ferreira e Araújo (2006) a função básica da Segurança da Informação é proteger o ativo de informação, minimizando os riscos a níveis aceitáveis.

A segurança da informação é uma necessidade das empresas para travar uma batalha pelos riscos que a informação fica exposta. Riscos esses que são em tempo real e um pequeno descuido podem gerar transtornos com graves conseqüências para a empresa e para os negócios, pois a todo minuto se criam novas formas de ataque, invasão, vírus, entre outros.Dessa forma, quando se fala em Segurança de Informação todo o esforço para proteger os dados, estabelecer processos de controle e prevenir riscos é sempre pouco.

Segurança de Informação relaciona-se com múltiplos e desiguais aspectos relativos a confidencialidade, integridade e disponibilidade da informação. Esses três termos caracterizam a preservação da mesma e de acordo com (Sêmola, 2003) podem ser definidos da seguinte maneira:

1. Confidencialidade: Toda informação deve estar segura de que será acessada somente pelas pessoas a quem ela se destina.

2. Integridade: Toda informação deve estar protegida e isenta de erros, ou seja, na exatidão em que a mesma foi disponibilizada. Visando também a proteção contra eventuais alterações acidentais ou intencionais.

3. Disponibilidade: Toda informação deverá estar disponível aos seus usuários autorizados quando eles solicitarem e com a freqüência que necessitarem.

É importante ressaltar que a segurança aplicada nas informações não está restrita a sistemas computacionais, informações eletrônicas ou qualquer outra forma mecânica de armazenamento. Ela se aplica a todos os aspectos de proteção e armazenamento de informações e dados, em qualquer forma, sejam elas em papel, em algum tipo de mídia ou arquivo.

Alguns termos, que são aplicados à segurança da informação, segundo (Sêmola, 2003), são descritos a seguir:

1. Informação: ativo de altíssimo valor nas corporações e que requer grande proteção de acordo com o seu coeficiente de valor.

2. Ativo: a informação em si, ou qualquer componente que compõe os processos que interferem direta ou indiretamente o fluxo da informação na empresa desde a sua origem até o seu destino. Exemplos: equipamentos computacionais, sistemas, manuais, ferramentas de desenvolvimento, mídias, serviços gerais (iluminação, eletricidade,...), entre outros.

3. Ameaças: condições que podem causar incidentes por meio da descoberta de vulnerabilidades.

4. Vulnerabilidades: são "brechas" que podem abrir caminho para uma ameaça ocorrer.

5. Impactos: decorrência de uma vulnerabilidade ter sido descoberta por uma ameaça.

6. Riscos: são as probabilidades das ameaças descobrirem as vulnerabilidades e conseqüentemente causar impactos nos negócios.

A seguir são apresentados alguns procedimentos de segurança necessários à organização.

2.4 Procedimentos de segurança

Antes de qualquer atitude é importante observar que os riscos encontram-se fora e dentro do ambiente da empresa, ou seja, ao mesmo tempo em que é imprescindível tomar precauções contra os ataques externos, não se pode deixar de levar em conta que os riscos também ocupam espaço dentro da organização. Entretanto a necessidade da conscientização

dos funcionários quanto à implantação de novas regulamentações, tecnologias e práticas de segurança é outro fator importante.

Os usuários muitas vezes não têm a devida noção da importância da informação, deixando que elas vazem, por exemplo. O prejuízo causado quando informações confidenciais são utilizadas indevidamente é algo que não pode ser medido, pois as implicações acabam por atingir a imagem da empresa.

Os impactos causados pelos riscos podem ser evitados por medidas de segurança, porém é indispensável ter consciência de que o risco nunca poderá ser nulo, isto é, por mais que a organização esteja em conformidade com relação a práticas de segurança, as chances de a mesma sofrer algum ataque é inteiramente possível.

Diante disso, pode-se concluir que os riscos são individuais e sempre será necessário avaliá-los para poder aplicar a devida porção de segurança.

Os mecanismos de segurança trabalham para evitar ou minimizar a possibilidade de ocorrência de eventuais riscos decorrentes de falhas ou deficiências nos processos internos, pessoas e sistemas, e também de fatores externos que são capazes de gerar perdas ou afetar negativamente a organização.

Alguns exemplos dessas medidas são: análise de riscos, câmeras de vídeo, palestras de conscientização e políticas de segurança.

Por fim, toda essa prudência serve para prevenir, detectar ou então corrigir a informação e seus ativos sempre com o intuito de impedir que as ameaças explorem vulnerabilidades e causem impactos nos negócios.

A seguir são apresentados os principais aspectos a serem considerados para o sucesso da implantação da Segurança da Informação nas organizações.

2.5 Principais aspectos para o sucesso da implantação da Segurança da Informação – o cuidado é de todos

O processo de implantação da Segurança da Informação em uma empresa não é simples e envolve muitos aspectos. Para que esta ação seja satisfatória, depende fatalmente de um alto grau de comprometimento de todos para que a empresa possa ser recompensada.

As pessoas envolvidas precisam estar cientes que cada informação obtém a sua classificação e salvaguarda, e também, que cada uma delas tem o seu acesso permitido, isto é, os indivíduos que compõe a organização devem estar atentos em relação aos graus de importância das informações. Tudo isso para garantir a impossibilidade de pessoas não autorizadas obterem informações indevidas durante o acesso, o armazenamento, o transporte e o descarte das mesmas.

Nesse sentido, é extremamente importante que todos os membros da empresa tenham extremo cuidado e prestem a máxima atenção ao abordar informações, porque podem conter dados estratégicos ou confidenciais, e cair em mãos erradas.

Para alcançar esta esperada conscientização é indispensável que a alta administração da empresa eduque os usuários com a intenção de evitar o mau uso das informações, seja por meio de cursos, treinamentos ou participação em palestras, ou seja, informando as políticas de segurança que serão adotadas, afinal o importante é assegurar que as informações contidas no ambiente não sejam acessadas antes dos usuários passarem por esses treinamentos.

Mas o que são essas políticas de segurança? Essas políticas servem para criar uma harmonia dentro da empresa, e sua adoção é necessária. Política de segurança é basicamente um documento que descreve as atividades dos usuários, dando a noção de quais informações da empresa eles estão autorizados a manipular, além de especificar a maneira, o lugar e o momento em que eles podem utilizar tais informações. Esse manual é de essencial seriedade

na empresa e deve contar com o apoio da alta administração para que as regras impostas sejam desempenhadas com perfeição e será abordado em mais detalhes no capítulo 5.

Após os treinamentos os usuários estarão aptos para agir de forma correta no ambiente da empresa.

Embora sejam realizados investimentos em recursos humanos, é indispensável que os usuários colaborem incessantemente com as regras adotadas, para que sejam capazes de acompanhar o desenvolvimento da empresa, pois planos e estratégias bem estruturados só conseguem ser implementados se tiverem um time de profissionais bem treinados, motivados, satisfeitos e principalmente interessados em aprender. Dessa forma, a partir do momento que a segurança da informação tornar-se parte da cultura da empresa, cada funcionário deve cumprir o seu devido papel dentro da organização, de acordo com as conformidades que serão estabelecidas e ajudar a empresa na sua busca pela constante melhoria.

A seguir são apresentadas algumas considerações sobre o aumento da Segurança da Informação nas organizações.

2.6 Crescimento de Segurança da Informação nas empresas

Plano de negócios, análise de mercado, metas a serem atingidas e estratégias a serem adotadas, nada disso irá fluir se os mesmos não estiverem aliados a uma gestão de segurança da informação apropriada. Não existe negócio sem risco e é preciso saber conviver com eles e fazer com que a empresa saiba administrá-los com competência. Nenhuma organização terá sucesso se não defender a segurança de suas informações, pois impulsiona o andamento da empresa em todos os seus departamentos, e é justamente por este fato que dia-a-dia se torna mais imperativa as atenções para as questões relacionadas a segurança da informação.

O crescimento de uma organização também depende da imagem que ela representa no mercado, e uma boa imagem é fundamental para conquistar e manter novos espaços no mercado, e é por esse e vários outros motivos, como o aumento de produtividades dos usuários, redução dos custos provocados pelas ameaças e pela má utilização dos recursos tecnológicos, entre outros, que a implantação de métodos de segurança da informação irá refletir potencialmente no ambiente externo.

Caso a empresa não tenha adotado políticas de seguranças, definindo o grau de importância da informação e delimitando o seu acesso, as informações podem estar a qualquer momento nas mãos dos concorrentes, funcionários internos não autorizados e *hackers*. Diante disso, é fácil perceber a importância da aplicação da segurança da informação nas empresas, ou seja, somente com o emprego desta ação a empresa estará protegida com relação aos riscos, podendo identificá-los, enfrentá-los e evitá-los, para que os mesmos não possam vir a comprometer o alcance dos objetivos de negócio da organização. Além de causar prejuízos financeiros e danos à imagem da empresa, os riscos impedem que a meta do crescimento seja atingida, por isso, as atitudes de prevenção são fundamentais no combate aos impactos dos negócios.

A segurança também esta relacionada à produtividade, porque a partir do momento que a empresa conseguiu identificar suas ameaças e seus pontos vulneráveis, e aplicou as eficientes ações de proteção nas suas informações, os usuários passam a trabalhar em um ambiente altamente organizado e isso influenciará substancialmente na produção, obtendo maior controle sobre os recursos disponíveis.

Entretanto, além de garantir a credibilidade e a imagem da organização, é importante reconhecer que a gestão da segurança da informação faz parte de um processo ininterrupto e constante dentro da organização.

A seguir são apresentados os benefícios com os investimentos em segurança. Infelizmente, muitos empreendedores ainda acreditam que os recursos utilizados na segurança das informações são “gastos”. Mas isso tende a mudar.

2.7 Por que investir em segurança? Quais os benefícios?

O mundo globalizado de hoje, complexo e competitivo, exige vários cuidados, e o principal deles é a segurança e é por isso que independente do tipo e do tamanho da organização, o investimento em segurança da informação é obviamente necessário.

O termo segurança está longe de ser uma palavra vaga e distante, ela não representa somente uma necessidade e sim uma obrigação, ou seja, é o ingrediente prioritário que impulsionará a empresa em busca do seu desenvolvimento.

Mas antes de começar a investir é preciso que a empresa considere quais são seus objetivos, iniciando-se com um diagnóstico da atual situação financeira, realizando um planejamento cuidadoso, pois no mercado atual as empresas estão com seus orçamentos cada vez mais curtos e cada gasto deve ser justificado. Além disso, é necessário investir de acordo com a criticidade das ameaças e das vulnerabilidades que podem causar impactos nos negócios da empresa.

O processo de segurança é um processo de realimentação, que envolve pessoas, equipamentos, sistemas e entre outros processos, a grande importância em investir ainda é uma questão que traz diversas dúvidas. Proteger informações não é sinônimo de luxo e muito menos de uma ação de baixa prioridade, e muitos executivos desconhecem as ameaças e as vulnerabilidades que a empresa está sujeita constantemente. Eles ainda não sabem ao certo, quanto, como e onde investir em segurança.

Nesse sentido, a questão é refletir em quanto a empresa pode perder se não investir e não em quanto ela vai lucrar, ou seja, o *ROI (Retorn of Investiment)* da segurança não tem uma dimensão definida, a questão de investimento está intimamente ligada ao diferencial competitivo que é algo estável, e uma vez que a empresa apresentar uma gestão de processo de segurança bem estabelecida, certamente ela atrairá novos clientes e originará mais lucros.

De acordo com um artigo publicado no site da TRUE ACCESS (2004), Cristiane Pereira (consultora de segurança da informação da *True Access Consulting),* define alguns benefícios da aplicação da segurança da informação nas empresas:

- Diferencial competitivo:

A concorrência é um fato indiscutível e irreversível. Dessa forma, se a estratégia de segurança aplicada for bem sucedida, a empresa poderá produzir com qualidade e segurança, além disso, poderá superar os seus concorrentes e sinalizar credibilidade ao mercado. Além da manutenção dos clientes atuais, com uma boa imagem na mídia a organização poderá aproximar clientes potenciais.

- Redução de riscos

Entre todos os benefícios da aplicação da segurança nas empresas este é o mais evidente, ou seja, a partir do momento que a empresa começar a tomar certos cuidados com a exposição e manipulação de informações, ela certamente reduzirá a ocorrência dos riscos. Por exemplo, vazamentos, roubo de informações, uso indevido e qualquer outro problema relacionado aos princípios básicos da informação que são a confidencialidade, a disponibilidade e a integridade.

- Diminuição de incidentes de segurança da informação e comprometimento de ativos

Com a implantação de procedimentos preventivos, os ativos não serão afetados e os imprevistos de segurança serão minimizados.

- Pessoal atento à segurança

A necessária realização do processo de segurança só poderá ser bem praticada se tiver por trás um time de profissionais bem treinados, motivados e satisfeitos, conseqüentemente, essa integração do pessoal junto com a segurança resultará em bons resultados.

- Clientes e fornecedores com alto nível de segurança

Manifestação de respeito e confiança para clientes e parceiros de negócio também é uma das vantagens desse investimento, pois, demonstrará seriedade e relevância da empresa com relação aos seus negócios.

- Direcionamento das diversas áreas da empresa para a execução fiel da segurança da informação em seus negócios

Com a segurança da informação, haverá um maior controle nos processos nas diversas áreas da empresa e um fácil acesso aos dados. Isso possibilitará que a informação chegue no seu real destino com eqüidade e com a preservação de interesses confidenciais e sigilosos.

- Decisões melhor embasadas

Quanto mais eficaz for a solução de segurança na empresa, as tomadas de decisões serão mais bem embasadas, novas aplicações de negócio serão viabilizadas mais rapidamente existindo assim um alinhamento de suas ações às melhores práticas de mercado.

Uma coisa é certa, segurança da informação é uma gestão que está em ebulição e quaisquer que sejam os inúmeros benefícios que a organização obterá com a implantação da segurança, o mais importante é a sua melhoria a qual deverá ser buscada continuamente, pois somente com o constante aperfeiçoamento, a empresa conseguirá o reconhecimento e o sucesso aos olhos do mercado.

A seguir serão abordados os principais componentes da Segurança da Informação.

3 COMPONENTES DA SEGURANÇA DAS INFORMAÇÕES

Os componentes da segurança da informação são: os ativos, as ameaças, as vulnerabilidades e os riscos, que serão descritos a seguir.

3.1 O que é ativo?

Ativo é tudo aquilo que de alguma maneira possui valor para a empresa e como tudo o que tem valor precisa ser bem protegido. Ativos são os elementos que a segurança da informação busca proteger devido a sua importância para as corporações.

O valor do ativo pode ser o próprio ativo fisicamente, por exemplo, um servidor (hardware), como também pode ser que o mesmo não seja palpável, mas o seu valor seja imensamente maior do que diversos outros ativos que são físicos dentro da empresa, podendo citar em muitos casos os dados e informações contidos nos bancos de dados das empresas.

Os ativos evoluíram e deixaram de ser a terra e os bens de produção para serem bens intangíveis como marcas, processos, banco de dados e tecnologias. Por conta disso, ganha importância a proteção dos ativos intangíveis, uma vez que na evolução da antiga economia industrial para a economia digital, o patrimônio físico e tangível como máquinas e terrenos deixaram de ser o principal gerador de valor.

Atualmente, o principal elemento criador de riqueza é o conhecimento e todos os ativos por ele gerados direta ou indiretamente, sejam eles, propriedade intelectual, marcas, domínios, tecnologias, softwares, licenças, conteúdos, e compostos.

A seguir é apresentada uma classificação de ativos.

3.1.1 Classificação de ativos

Os ativos podem ser classificados por diversos aspectos. Segundo Sêmola (2003) os ativos podem ser divididos e agrupados de várias formas para facilitar o seu tratamento e um modelo pode ser o seguinte:

- Informações

Nesta categoria encontram-se as informações propriamente ditas, estejam elas armazenadas ou representadas de qualquer forma, em meio físico, eletrônico ou mesmo que sejam conhecimentos que estejam armazenados no cérebro de quem a possui.

Exemplos: documentos, relatórios, códigos de programação, arquivos de configuração, tabelas de custos de produtos, planilhas de remuneração de funcionários e muitos outros.

- Recursos que fornecem suporte a ela (informação);

Esta categoria pode ser dividida em outras três subcategorias para facilitar o estudo e entendimento da mesma.

a) Software

Este grupo de ativos contém todos os programas de computador utilizados para a automatização de processos, incluindo acesso, leitura, transmissão e armazenamento das informações.

De acordo com a Lei n° 9.609/98, de 19 de fevereiro de 1998, Capítulo 1 e artigo 1º, Programa de Computador é definido como:

> "É a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados."

A segurança da informação busca avaliar a maneira pela qual as aplicações são concebidas, disponibilizadas e utilizadas pelos usuários e por outros sistemas para detectar e corrigir problemas existentes em seu funcionamento ou na forma que se comunicam. Alguns exemplos de softwares: Sistemas Operacionais, aplicativos, soluções *ERP* (*Enterprise Resource Planning*), *CRM* (*Customer Relationship Management*) e outros softwares instalados nos computadores da empresa.

b) Hardware

Este grupo de ativo representa todos os elementos físicos dos sistemas computacionais que oferecem suporte ao processamento, armazenamento e transmissão das informações.

A segurança da informação busca avaliar quais tipos de ameaças podem afetar este tipo de ativo, para que assim possa protegê-los. As principais ameaças para este tipo de ativo são: falhas elétricas que danifiquem os equipamentos, inundações em centros de computação, roubo de computadores portáteis, entre outros. Alguns exemplos de hardware são: computadores pessoais (PC's), servidores, laptops, mídias de armazenamento, *hubs* e *switchs.*

c) Organizacional

Neste grupo estão inclusos todos os aspectos que compõem a estrutura física e organizacional da empresa.

A segurança da informação busca proteger a empresa de ameaças que os próprios colaboradores oferecem a ela, como: acesso indevido a locais restritos ou utilização dos recursos da empresa para fins particulares. Alguns exemplos de organizacional são: estrutura departamental, hierarquia, CPD (Central de Processamento de Dados), etc.

- Pessoas que a utilizam (usuários)

Neste grupo refere-se aos usuários, ou seja, os indivíduos que lidam com as informações no seu dia-a-dia de trabalho.

O enfoque da segurança das informações nos usuários está voltado para a formação de consciência sobre segurança, para que estes tomem decisões e empreendam ações de acordo com as necessidades de proteção. Isso vai desde a alta direção até os usuários finais da informação, incluindo os grupos que mantêm em funcionamento a estrutura tecnológica, como técnicos, operadores e administradores. Dentro desta categoria podem ser enquadradas praticamente todas as ameaças de origem humana, de roubo e invasões.Alguns exemplos de organizacional são: funcionários, profissionais terceirizados e executivos.

A seguir são apresentadas possíveis falhas na Segurança de Informação, ou seja, as ameaças.

3.2 Ameaças

As ameaças são eventos capazes de explorar as falhas de segurança, que são denominadas vulnerabilidades. Como conseqüências, provocam danos aos ativos da empresa ou situações não planejadas, afetando os seus negócios em ambos os casos por conta dos prejuízos causados.

Os ativos estão constantemente sob ameaças que podem colocar em risco a integridade, a confidencialidade e a disponibilidade das informações. Essas ameaças sempre existirão e estão relacionadas a causas que raramente as empresas controlam.

Dessa forma, entende-se que um dos objetivos da segurança da informação é impedir que as ameaças explorem as vulnerabilidades e afetem um dos princípios básicos da segurança da informação (integridade, disponibilidade, confidencialidade), provocando danos ao negócio das empresas.

As ameaças são freqüentes e podem ocorrer a qualquer momento. Essa relação de freqüência-tempo se baseia no conceito de risco, o qual representa a probabilidade de que uma

ameaça se concretize por meio de uma vulnerabilidade, combinada com o impacto que a ameaça irá causar, e pode ser classificada em três grupos:

1. Ameaças naturais - condições da natureza que poderão provocar danos nos ativos. Por exemplo: fogo, inundação, terremotos, entre outros.
2. Intencionais - são ameaças deliberadas causadas por pessoas. Por exemplo: fraudes, vandalismo, sabotagem, espionagem, invasão e furto de informações, entre outros.
3. Involuntárias - são ameaças resultantes de ações inconscientes de usuários, muitas vezes originadas pela falta de conhecimento no uso dos ativos. Por exemplo: erros e acidentes.

Algumas ameaças às informações, como: vírus, *spam*, *trojan* ou cavalo de tróia, funcionários insatisfeitos, furto e quebra de senhas, vazamento de informação, *hacker*, falha de segurança interna, são descritas a seguir.

3.2.1 Vírus

Os vírus são pequenos segmentos de códigos programados, normalmente com más intenções, que têm a característica de se agregar ao código de outros programas. Assim que são executados, disparam o código maliciosamente alterado a fim de causar modificações indevidas no processamento normal do sistema em que este se encontra, causando danos leves a danos irreparáveis.

De acordo com (Dias, 2000), os vírus podem ser classificados, da seguinte maneira:

- Vírus de arquivos ou programas: infectam arquivos de programa. Esses arquivos normalmente têm extensões como: *.COM, .EXE, .OVL, .DLL, .DVR, .SYS, .BIN.*

- Vírus de setor de boot: infectam a área do sistema de um disco, ou seja, o registro de inicialização em disquetes e discos rígidos. Todos os disquetes e discos rígidos (incluindo discos com dados apenas) contêm um pequeno programa no registro de inicialização que é executado quando o computador é iniciado. Os vírus de setor de boot anexam-se a esta parte do disco e são ativados quando o usuário tenta iniciar a parte do disco infectado. Exemplos de vírus de setor de boot são *Form, Disk Killer, Michelangelo e Stoned.*
- Vírus de macro: infectam os arquivos dos programas *Microsoft Office Word*, *Excel*, *PowerPoint* e *Access*. Variações mais recentes também estão aparecendo em outros programas. Todos estes vírus usam a linguagem de programação interna do programa, que foi criada para permitir que os usuários automatizem determinadas tarefas neste programa. Devido à facilidade com que estes vírus podem ser criados, existem milhares deles espalhados.
- Vírus *Multipartite*: infectam setores de boot, disquetes e arquivos executáveis. Exemplo: *Dead.Boot*.488, *Pieck*.4444.A, *Delwin*.1759.
- Vírus Polimórficos: utilizam técnicas de criptografia para construir a seqüência de *bytes* de seu corpo. A cada cópia gerada, uma nova combinação é utilizada para criptografar essa seqüência. De forma que um único vírus pode ter inúmeras formas diferentes, que são decodificadas por chaves contidas em uma pequena parte do vírus, sempre que necessário. Exemplo: *Satan Bug*, *Spanska.4250*, *W95/HPS*;
- *Worms*: São programas maliciosos semelhantes aos vírus, porém se diferenciam na forma de infecção. Os *Worms* somente fazem cópias deles próprios e as propagam. Exemplo: *LittleDavinia, LoveLetter, Navidad.*

3.2.2 SPAM

Spam são mensagens eletrônicas não solicitadas enviadas em massa. Sua forma mais popular consiste numa mensagem de correio eletrônico com fins publicitário. Quando o conteúdo é exclusivamente comercial, este tipo de mensagem também é referenciada como *UCE* (do inglês *Unsolicited Commercial E-mail*).

Os usuários do serviço de correio eletrônico podem ser afetados de diversas formas, tais como:

- Gasto desnecessário de tempo: para cada *spam* recebido, o usuário necessita gastar um determinado tempo para ler, identificar o e-mail como *spam* e removê-lo da caixa postal.

- Perda de produtividade: para quem utiliza o e-mail como uma ferramenta de trabalho, o recebimento de *spams* aumenta o tempo dedicado à tarefa de leitura de e-mails, além de existir a chance de mensagens importantes não serem lidas, serem lidas com atraso ou apagadas por engano.

- Prejuízos financeiros causados por fraude: o *spam* tem sido amplamente utilizado como veículo para disseminar esquemas fraudulentos, que tentam induzir o usuário a acessar páginas clonadas de instituições financeiras ou a instalar programas maliciosos projetados para furtar dados pessoais e financeiros. Este tipo de *spam* é conhecido como *phishing*. O usuário pode sofrer grandes prejuízos financeiros, caso forneça as informações ou execute as instruções solicitadas neste tipo de mensagem fraudulenta.

3.2.3 *Trojan* ou Cavalos de Tróia

Trojans ou Cavalos de Tróia são programas executáveis que transformam seu micro em um terminal de Internet aberto. Estes programas eliminam as proteções que impedem a

transferência de informações, ou seja, abrem uma porta de comunicação (*backdoor*) não monitorada.

Um programa de cavalo de tróia funciona como um servidor de rede (*Server*) e tem um outro programa comparsa, que funciona como cliente (*CLIENT*). O *server* fica no seu computador e o *client* fica no computador do *cracker* (é o termo usado para designar quem quebra um sistema de segurança, de forma ilegal ou sem ética). Se ambos estiverem na internet, o *cracker* pode estabelecer uma conexão direta (cliente-servidor), não monitorada e imperceptível com o *Server* (você) por meio de uma *backdoor*. Uma *backdoor* (cuja tradução literal é porta de trás) é apenas um canal de comunicação identificado por um número.

As formas mais comuns de receber *trojans* são por meio de e-mails (com executáveis ou arquivos camuflados) e por meio de outros programas, geralmente jogos.

3.2.4 Funcionários insatisfeitos

Grande parte das invasões realizadas nas empresas tem participação de funcionários ou ex-funcionários.

A informática e a tecnologia facilitam muito essas atividades, ou seja, um funcionário pode copiar o equivalente a uma sala de documentos em um *pen drive* e sair da empresa com este acessório no bolso. Um funcionário insatisfeito com a empresa também pode acrescentar uma cópia oculta, destinada ao concorrente, toda vez que enviar uma proposta comercial para os clientes da organização. E igualmente, um funcionário descontente pode acessar uma informação estratégica da empresa, ou até mesmo ou um conjunto delas e apagá-las, e com esse domínio poderá divulgar o plano de negócio da empresa prejudicando a mesma no mercado.

3.2.5 Furto e quebra de senhas

O arquivo de senha roubado de um servidor é submetido à quebra por uma ferramenta de *crack* de senha. Assim são obtidas as senhas dos usuários que tiveram seu servidor invadido.

Um *cracker* de senha é qualquer programa que supera a segurança da senha revelando senhas que foram criptografadas, porém, isto não significa que o *cracker* de senha possa necessariamente desencriptar qualquer coisa. De fato a grande maioria dos *crackers* de senha não consegue fazer isso. Em geral, não se pode desencriptar senhas com algoritmos fortes, pois eles possuem chaves difíceis de serem descobertas.

3.2.6 Vazamento de informação

O vazamento remoto de informações é obtido por meio da resposta a consulta de *Ping, Traceroute, Telnet, SNMP*, etc. A coleta de informações relativas à versões de sistemas operacionais e *hosts* dão ao invasor informações que o permitirá planejar seu ataque à rede.

3.2.7 *Hacker*

É aquela pessoa que possui uma grande facilidade de análise, assimilação, compreensão e capacidades surpreendentes de conseguir fazer o que quiser (literalmente) com um computador. Ela sabe perfeitamente que nenhum sistema é completamente livre de falhas, e sabe onde procurar por elas, utilizando técnicas das mais variadas (aliás, quanto mais variado, mais valioso é o conhecimento do *hacker*).

3.2.8 Falha de Segurança Interna

As ameaças internas podem ser consideradas como o risco à segurança dos recursos computacionais. Um bom programa de segurança física é o passo inicial para a defesa da corporação no sentido de proteger as suas informações contra acessos indevidos. Este programa deve iniciar no decurso da realização de uma análise de risco.

Os seguintes elementos devem ser checados durante esta análise: portas das salas trancadas, mesas e armários trancados, estações de trabalho protegido contra acessos indevidos, disposição e proteção das mídias magnéticas de armazenamento, cabeamento de rede padronizado e seguro, informações protegidas (em meio magnético e papel), documentos sobre as mesas, descarte de informações (se existem trituradoras de papéis), áreas de circulação de visitantes a áreas restritas.

Uma lista das principais ameaças de segurança física poderia conter os seguintes itens: incêndio (fogo e fumaça), água, (vazamentos, corrosão, enchentes), tempestades, vandalismo, roubos, furtos, construções próximos a equipamentos de tecnologia, materiais tóxicos, falhas em equipamentos, interrupção de energia, entre outros.

A seguir são apresentadas algumas estatísticas sobre as ameaças na segurança da informação.

3.2.9 Estatísticas de ameaças

Foi realizado um estudo no ano 2003 pela Módulo S.S.S.A, das principais ameaças de segurança da informação no Brasil. A metodologia utilizada contou com a coleta de dados em (2003), onde contou com respostas presenciais via on-line. No total, a pesquisa

quantitativa teve uma amostra de 682 questionários, coletados entre março e agosto de 2003, junto a profissionais ligados às áreas de Tecnologia e Segurança da Informação.

Os profissionais que participaram deste estudo estão distribuídos em diversos segmentos, como: Financeiro (21%), Governo (17%), Indústria e Comércio (14%), Tecnologia/Informática (14%), Prestação de Serviços (9%), Outros (8%), Telecomunicações (7%), Comércio/Varejo (4%), Energia Elétrica (2%), Educação (2%) e Saúde (2%), correspondendo à cerca de 50% das 1000 maiores empresas brasileiras.

Essas ameaças são apresentadas a seguir.
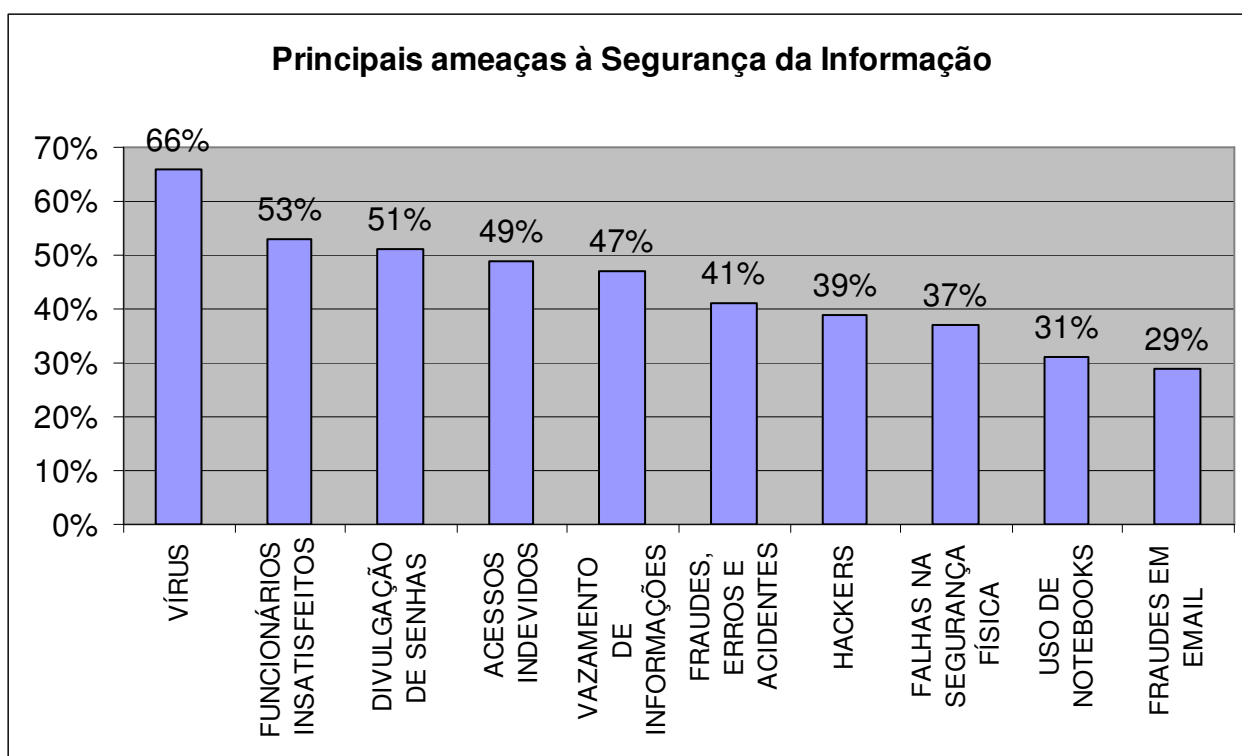
Figura 1: Principais ameaças à Segurança da Informação

Fonte: (Módulo *Security*)

Dentre as principais ameaças que afetam as empresas, os vírus representam a maior fatia de proporção.

A seguir são apresentados os valores acumulados de SPAM de 2003 a 2006 (agosto), segundo CERT.br.
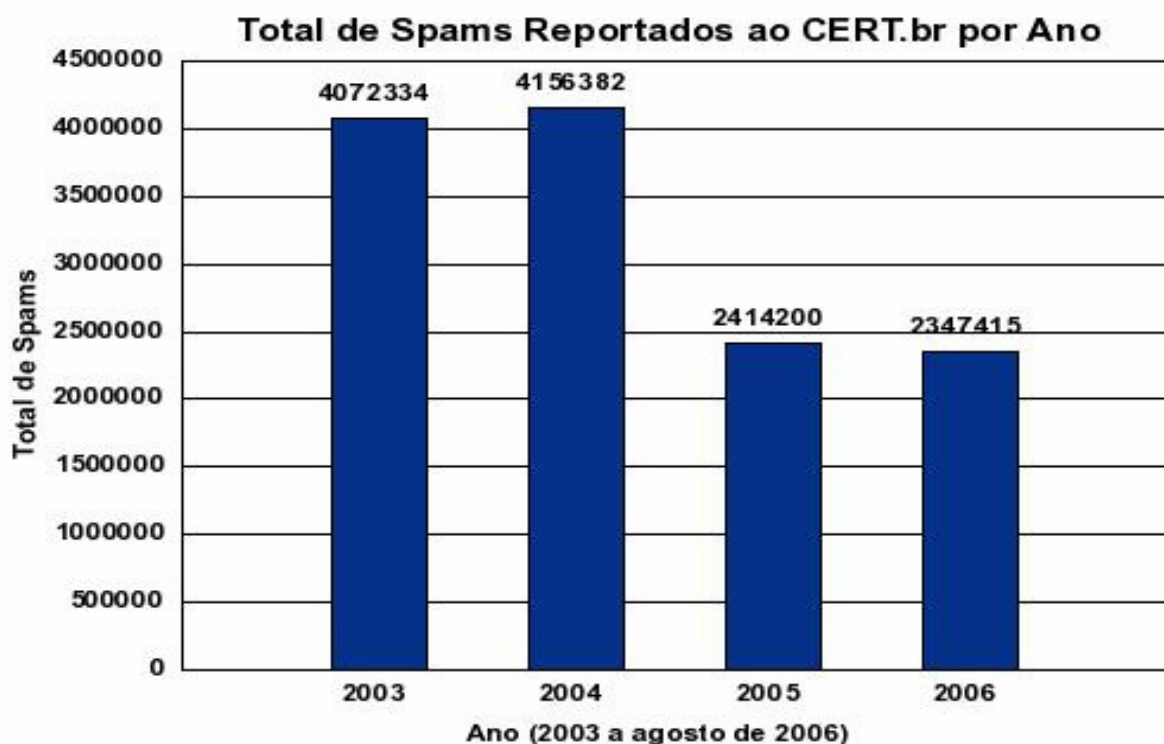
Figura 2: Total de *Spams* citados pelo CERT.br por ano

Fonte: (Cert.br Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil)

Nota-se que no período de 2003 até 2006 reduziu-se expressivamente o total de *spam*.

A seguir são apresentados os incidentes por dia da semana.
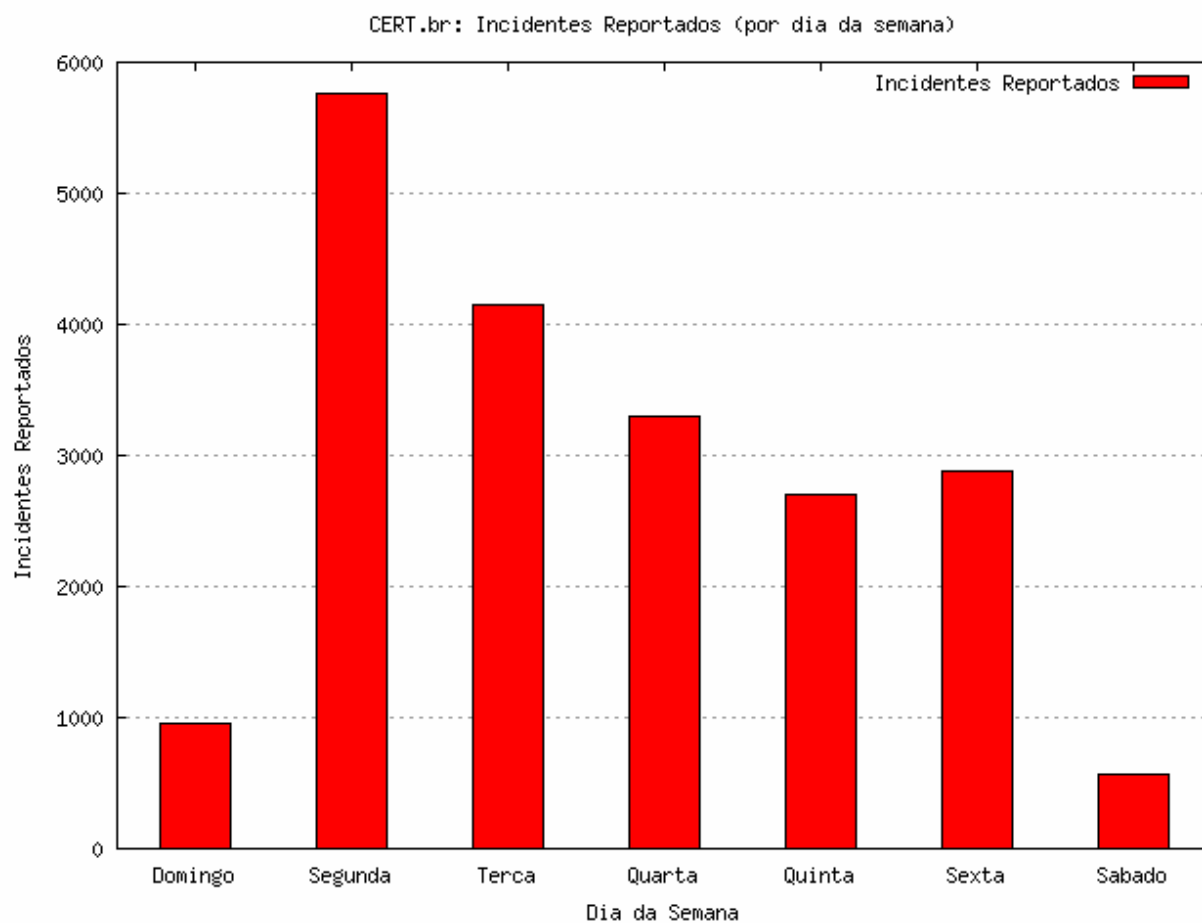
Figura 3: Incidentes por dia da semana

Fonte: (Cert.br Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil)

Nota-se que o pico está na segunda-feira, ou seja, os incidentes têm uma tendência maior de incidência no primeiro dia da semana.

A seguir são apresentados os incidentes reportados de Janeiro a Junho de 2006, que comprova os tipos de ataques e a sua ocorrência.
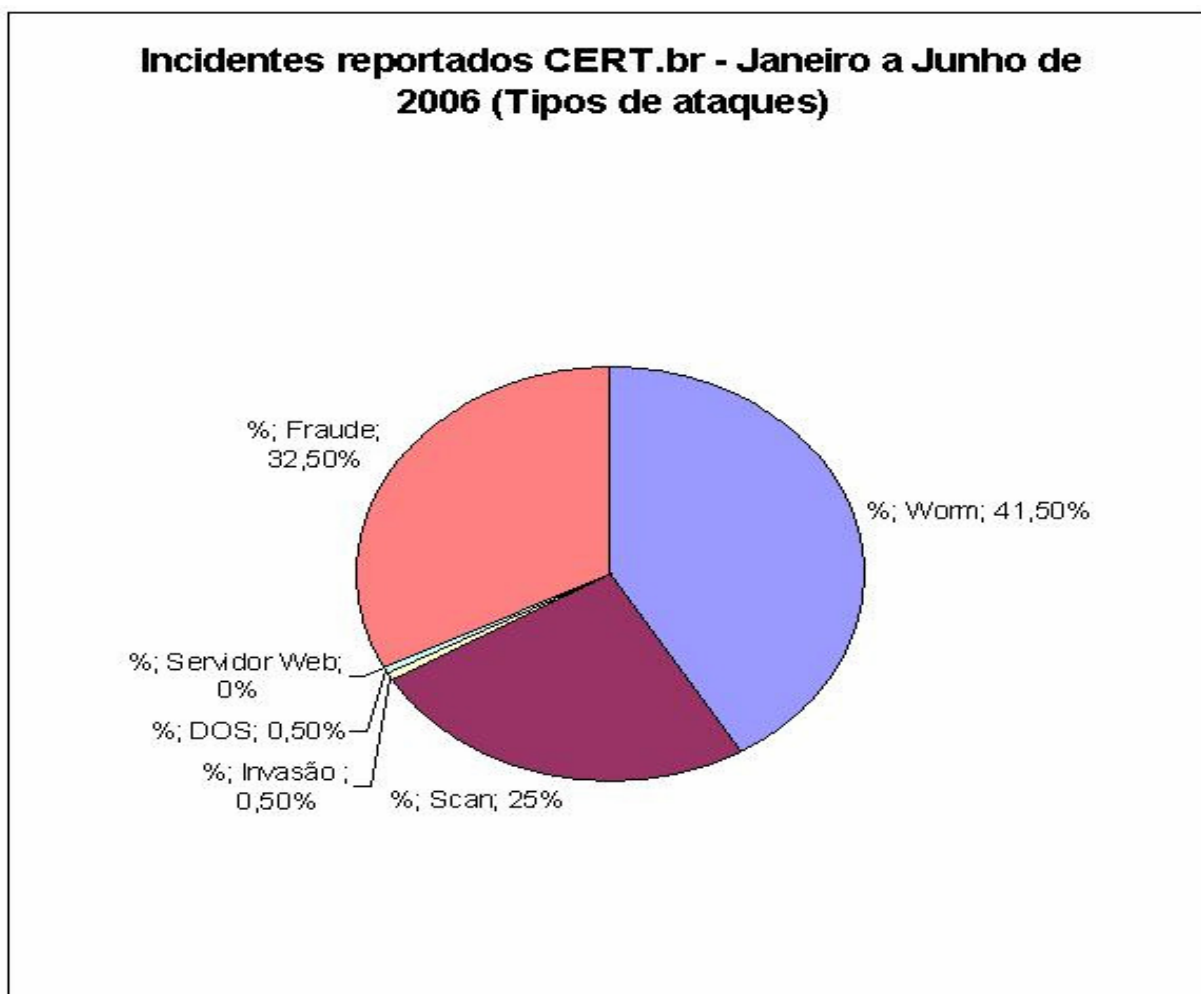
Figura 4: Ataques ocorridos no período de janeiro a junho de 2006

Fonte: (Cert.br Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil)

Observa-se que o ataque de que mais ocorreu neste semestre foi o causado por *Worm* com 41,50% e os ataques por meio de Servidor *web* foi nula.

A seguir são apresentados os incidentes no mundo.
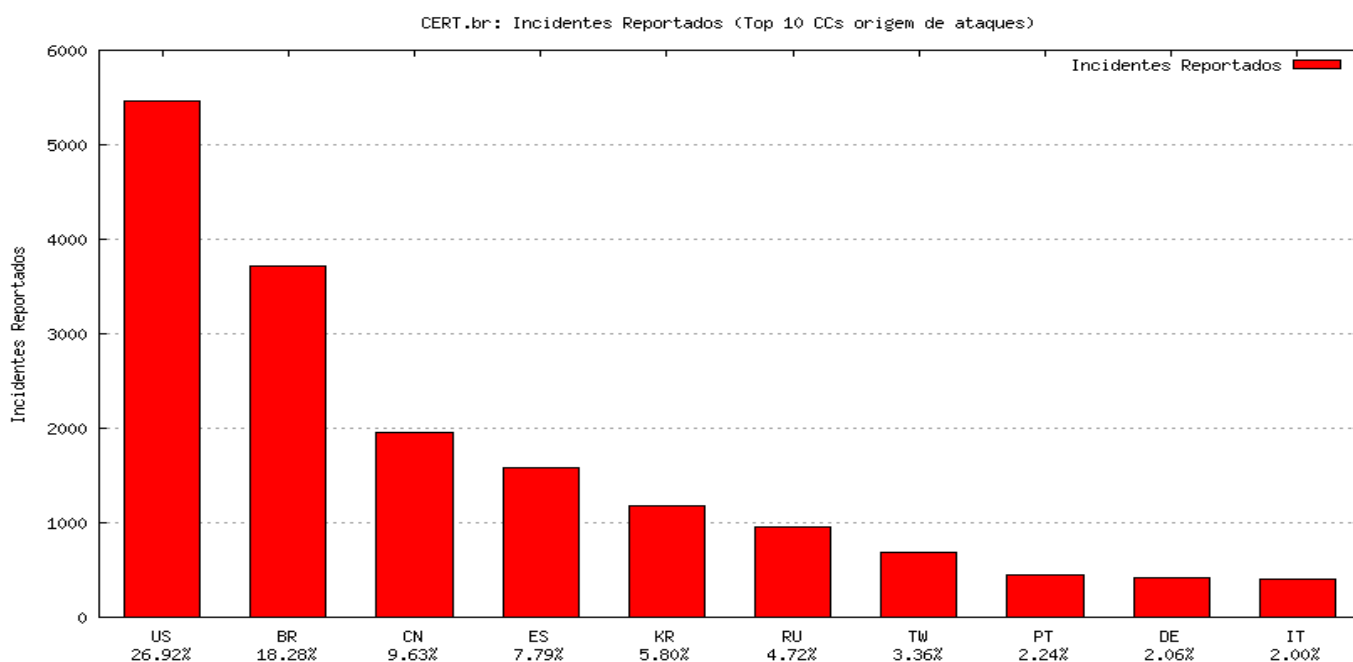
Figura 5: Incidentes no mundo

Fonte: (Cert.br Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil)

É possível observar os americanos ainda tem muita dificuldade de lidar com incidentes, representando o primeiro no ranking de 10 países. No entanto o Brasil ao mesmo tempo tem uma grande parcela de volume vindo em segundo lugar no ranking.

Diante dessas estatísticas, nota-se que as empresas ainda falham muito na tarefa de resguardarem os seus dados. Entre as principais ameaças, a ocorrência de vírus, a insatisfação dos funcionários e a divulgação de senhas estão entre as mais freqüentes, logo, os vírus, representam a maior ameaça à segurança da informação nas empresas.

Com relação aos incidentes, eles são freqüentes, ou seja, podem ocorrer a qualquer hora e dia da semana, e o Brasil, por exemplo, está em segundo lugar no ranking da pesquisa com relação à ocorrência dos mesmos. No entanto, fica claro que com a importância estratégica que vem conquistando as tecnologias da informação, os prejuízos com as invasões,

incidentes, fraudes, *spams* e vírus ainda estão provocando a cada ano impactos nos negócios das empresas.

Portanto, as empresas hoje em dia devem ficar atentas principalmente aos perigos que resultam da presença e do uso da internet, e reconhecer que a importância da proteção dos dados para o sucesso do negócio é fundamental.

A seguir serão apresentadas algumas considerações importantes sobre vulnerabilidades.

3.3 Vulnerabilidades

As ameaças sempre existirão, por isso é de se esperar que, à medida que a tecnologia progrida, também surjam novas formas por meio das quais elas possam se concretizar, portanto, é importante conhecer a estrutura geral de como se classificam as vulnerabilidades que podem fazer com que essas ameaças causem impactos em nossos sistemas, comprometendo os princípios da segurança da informação.

As vulnerabilidades podem estar expostas na parte física, hardware, software, meios de armazenamento, comunicação e humanas.

As vulnerabilidades são situações que, ao serem explorados por ameaças, afetam a confidencialidade, a disponibilidade e a integridade das informações de um indivíduo ou empresa.

Um dos primeiros passos para a implementação da segurança é rastrear e eliminar as vulnerabilidades de um ambiente de tecnologia da informação. Ao se identificarem as vulnerabilidades, será possível dimensionar os riscos aos quais o ambiente está exposto e definir as medidas de segurança mais apropriadas e urgentes para o ambiente.

As vulnerabilidades dependem da forma que se organizou o ambiente em que se gerenciam as informações. A existência de vulnerabilidades está relacionada à presença de elementos que prejudicam o uso adequado da informação. Dessa forma, pode-se compreender agora outro objetivo da segurança da informação: a correção de vulnerabilidades existentes no ambiente em que se usam a informações, com o objetivo de reduzir os riscos as quais elas estão submetidas. Dessa forma, evita-se a concretização das ameaças.

A seguir é apresentada uma classificação de vulnerabilidades, de acordo com (Sêmola, 2003).

3.3.1 Classificação das Vulnerabilidades

3.3.1.1 Vulnerabilidades físicas

Os pontos fracos de ordem física são aqueles presentes nos ambientes em que estão sendo armazenadas ou gerenciadas as informações. Por exemplo: instalações inadequadas do espaço de trabalho, ausência de recursos para o combate a incêndios, disposição desorganizada dos cabos de energia e de rede, entre outros.

3.3.1.2 Vulnerabilidades de hardware

Os possíveis defeitos de fabricação ou configuração dos equipamentos da empresa que poderiam permitir que as informações ou os próprios equipamentos fossem atacados.

A falta de configuração de equipamentos de contingência poderia representar uma vulnerabilidade para os sistemas da empresa, pois permite que uma ameaça de indisponibilidade de serviços críticos se concretizasse mais facilmente.

Existem muitos elementos que representam vulnerabilidades do *hardware*, tais como: a ausência de proteção contra acesso não autorizado, a conservação inadequada dos equipamentos, etc.

3.3.1.3 Vulnerabilidades de software

As vulnerabilidades dos softwares se caracterizam normalmente por falhas de programação e permitem, entre outras coisas, que ocorram acessos indevidos aos sistemas de computador, inclusive sem o conhecimento de um usuário ou administrador de rede. A configuração e a instalação indevida dos programas de computador, que poderão levar ao uso abusivo dos recursos por parte de usuários mal-intencionados é um exemplo.

Às vezes, a liberdade de uso implica aumento do risco. Por exemplo: programas de e-mail que permitem a execução de códigos maliciosos, editores de texto que admitem a execução de vírus de macro, entre outros. Esses pontos fracos colocam em risco a segurança dos ambientes tecnológicos.

Os aplicativos são os elementos que fazem a leitura das informações e permitem que os usuários acessem determinados dados em diversas mídias e, por isso, se transformam no objetivo favorito dos agentes causadores de ameaças. Por exemplo: os programas utilizados para edição de texto e imagem ou para a automatização de processos e os que admitem a leitura de informações, como os navegadores de páginas da Internet.

Os sistemas operacionais, como *Microsoft Windows* e *Unix*, que oferecem a interface para o acesso ao *hardware* dos computadores, costumam ser alvo de ataques. Por meio destes ataques é possível realizar ataques de alta gravidade, que normalmente comprometem todo o sistema. Esses aplicativos são vulneráveis a várias ações que afetam sua segurança. Por

exemplo: a configuração e a instalação inadequadas, a ausência de atualizações para *bugs* já conhecidos, programação insegura, etc.

3.3.1.4 Vulnerabilidades dos meios de armazenamento

Os meios de armazenamento são os suportes óticos, magnéticos, e outros, utilizados para armazenar as informações. E se forem afetados por vulnerabilidades poderão sofrer danos ou se tornarem indisponíveis.

Entre os tipos de meios de armazenamento de informações que estão expostos, pode-se citar: *CD-ROMs*, fitas magnéticas e discos rígidos. Estas mídias também podem possuir vulnerabilidades que permitiriam a concretização de ameaças.

Se os suportes (cd-rom, disquetes, fitas magnéticas e discos rígidos) que armazenam as informações não forem utilizados de forma adequada, seu conteúdo poderá estar vulnerável a uma série de fatores que poderão afetar a integridade, a disponibilidade e a confidencialidade das informações. Alguns exemplos: falhas ocasionadas por mal funcionamento, uso incorreto, local de armazenamento em locais inadequados, entre outros.

3.3.1.5 Vulnerabilidades de comunicação

Este tipo de vulnerabilidade abrange todo o tráfego de informações. Onde quer que transitem as informações, seja por cabo, satélite, fibra óptica ou ondas de rádio, deve haver preocupações com segurança. O sucesso no tráfego dos dados é um aspecto fundamental para a implementação da segurança da informação. Assim, a segurança da informação também está associada ao desempenho dos equipamentos envolvidos na comunicação, pois se preocupa

com a qualidade do ambiente que foi preparado para o tráfego, tratamento, armazenamento e leitura das informações. Por exemplo, a ausência de sistemas de criptografia nas comunicações poderia permitir que pessoas alheias à organização obtivessem informações privilegiadas, a má escolha dos sistemas de comunicação para envio de mensagens de alta prioridade da empresa poderia fazer com que elas não alcançassem o destino esperado no prazo adequado ou que a mensagem fosse interceptada no meio do caminho.

3.3.1.6 Vulnerabilidades humanas

Essa categoria de vulnerabilidade relaciona-se aos danos que as pessoas podem causar às informações e ao ambiente tecnológico que lhes oferece suporte.

Os pontos fracos humanos podem ser intencionais ou não. Muitas vezes, os erros e acidentes que ameaçam a segurança da informação ocorrem dentro do ambiente empresarial. A maior vulnerabilidade é o desconhecimento das medidas de segurança adequadas que são adotadas por cada elemento do sistema, principalmente os membros internos da empresa.

Alguns exemplos graves são: a ausência de capacitação específica em segurança para a execução das atividades inerentes às funções de cada um, falta de consciência de segurança para as atividades de rotina, erros ou omissões.

A seguir serão apresentadas algumas considerações importantes sobre análise de riscos.

3.4 Análise de Riscos

Análise de risco é uma medida que busca avaliar qual a real probabilidade de que ameaças se concretizem utilizando as vulnerabilidades existentes, além de identificar os

possíveis impactos que possam ser causados. A análise de riscos tem como resultado uma lista de problemas que devem ser priorizados, uns dos principais objetivos é diagnosticar a situação da segurança da informação na organização e recomendar ações para cada vulnerabilidade mapeada.

Uma Análise de Risco bem realizada poderá garantir a confidencialidade, a disponibilidade e a integridade das informações nas empresas.

A tarefa da análise de riscos é identificar os processos comerciais da organização em que se deseja implementar ou analisar o nível de segurança da informação. Na definição do escopo do projeto de análise de riscos, delimita-se o universo dos ativos sobre os quais oferecerão suas recomendações, com base na relevância do processo para a empresa no intuito de alcançar os objetivos da organização. De acordo com (Sêmola , 2003), fazem parte de uma análise de risco:

Processos de Negócio: identificar junto aos gestores e colaboradores os Processos de Negócio existentes na Empresa.

Ativos: identificar os ativos que serão considerados na Análise de Risco: Pessoas, Infra-estrutura, Aplicações, Tecnologia e informações.

Vulnerabilidades: identificar as vulnerabilidades existentes nos ativos que possam causar indisponibilidade dos serviços ou serem utilizadas para roubo das suas informações.

Ameaças: identificar os agentes que podem vir a ameaçar a empresa.

Impacto: tendo identificado as vulnerabilidades e ameaças, identificamos o impacto que estes podem causar na Empresa. Como roubo de informação, paralisação de serviços, perdas financeiras entre outros.

Ao definir o escopo, é importante considerar que os processos podem ser uma atuação da organização frente ao mercado, uma funcionalidade interna e externa, uma

atividade exercida, ou um produto elaborado, precisando de toda a organização para se tornar viáveis.

A seguir será abordada a análise técnica de segurança, que é realizada na análise de riscos.

3.4.1 Análise técnica de segurança

A análise técnica de segurança representa um dos pontos-chave na análise de riscos da empresa. Como já mencionado anteriormente, as informações são, hoje em dia, um dos principais ativos nas empresas, e, deste modo essa análise indicará o nível de segurança com o qual se conta dentro da empresa atualmente.

Por meio desse *check-up*, que é um dos passos mais importantes da análise de riscos, são feitas coletas de informações sobre a forma em que os ativos foram configurados e como são administrados por seus responsáveis e também de como foram estruturados na rede de comunicação.

No processo de análise técnica de segurança busca-se identificar vulnerabilidades de segurança na utilização e manipulação dos ativos da empresa e neste processo são considerados diversos tipos de ativos. A seguir são apresentados os ativos tecnológicos a serem analisados quando se deseja monitorar as vulnerabilidades presentes através de erros de configuração ou desconhecimento das possibilidades de ataque:

a) Estações de trabalho

Dependem da forma como estão configuradas para evitar que os usuários (com freqüência de forma inconsciente) permitam a ocorrência das ameaças.

Entre os exemplos de vulnerabilidades comuns desse tipo de ativos estão:

- Ausência de protetor de telas bloqueado por senha, permitindo que as máquinas deixadas sozinhas sejam utilizadas por pessoas não-autorizadas;
- Ausência de configurações de segurança permitindo a instalação ou execução de arquivos maliciosos;
- Periodicidade de atualização dos programas antivírus, presença ou ausência de documentos confidenciais;
- Forma de utilização da estrutura de servidores de arquivos, que garantam de uma maneira mais eficiente o *backup* dos dados, ou seja, sua disponibilidade.

b) Conexões

As conexões de comunicação entre as redes devem estar seguras: fibra óptica, satélite, rádio, antenas, etc. Para isso, é importante realizar atividades de análise sobre a forma com que as conexões estão configuradas e dispostas na representação topológica da rede. Isso garante que a comunicação seja realizada em um meio seguro, criptografada, se for necessário, livre de possibilidades de rastreamento de pacotes ou mensagens, e também desvio de tráfego para outros destinos indesejados.

c) Aplicativos

Os aplicativos são os elementos que fazem a leitura das informações de um processo de negócio ou de uma organização. Dessa forma, constituem um elemento muito importante, pois fazem a interface entre diversos usuários e diversos tipos de informação no que se refere a confidencialidade, integridade e disponibilidade. Dessa forma, os aplicativos devem garantir um acesso restritivo, com base nos privilégios de cada usuário e às informações que eles manipulam. Além disso, devem garantir também que suas configurações estejam de acordo com os princípios de segurança estabelecidos (muitos dos quais são reconhecidos por organismos internacionais) com relação à disponibilidade das informações, à forma como o

aplicativo às lê, guarda e transmite, até à maneira como o aplicativo foi desenvolvido, como suas fontes são atualizadas e armazenadas, entre outros.

A seguir serão apresentadas algumas considerações sobre as normas e padronizações internacionais de segurança.

4 PADRONIZAÇÃO DE SEGURANÇA

4.1 Considerações Iniciais

Os esforços relacionados com a busca de melhores mecanismos para defender a segurança culminaram com a homologação da "Norma Internacional de Segurança da Informação" denominada ***ISO/IEC 17799:2000***. Esta norma trata da segurança das informações e não somente dos dados que trafegam pela rede ou que residem dentro de um sistema computacional.

A Norma de Segurança da Informação trouxe mais do que vários controles de segurança. Essa norma permitiu a criação de um mecanismo de certificação das organizações, semelhante às certificações ISO já existentes, ou seja, esta nova certificação conduz a organização a manipular os seus dados e os dados dos clientes, de forma segura, independente da forma que são armazenados.

A tendência é que a *ISO/IEC 17799* se torne cada vez mais importante para as empresas do mundo todo, pois além de garantir que suas informações internas estão sendo gerenciadas de forma segura. Além disso, a certificação proporciona uma grande vantagem competitiva que consiste em comprovar aos clientes e parceiros de negócio que a empresa trata segurança da informação de forma séria e possui controles adequados para proteger informações sob sua guarda.

Nesse capítulo será apresentado os termos, as definições e os objetivos dos principais controles da Norma ISO/IEC 17799.

4.2 Termos e Definições

A *NBR ISO/IEC 17799* considera que a segurança de um ambiente é caracterizada pela manutenção de três fatores primordiais:

d) Confidencialidade: o princípio da confidencialidade é respeitado quando apenas as pessoas explicitamente autorizadas podem ter acesso á informação.

e) Integridade: o princípio de integridade é respeitado quando a informação acessada está completa sem alterações e, portanto, confiável.

f) Disponibilidade: o princípio de disponibilidade é respeitando quando a informação está acessível, por pessoas autorizadas, sempre que necessário.

Afirmar que um ambiente é aderente à Norma de Segurança da Informação significa dizer que o mesmo utiliza os recursos adequados para garantir a Disponibilidade, Confidencialidade e a Integridade de suas informações.

No entanto, devem ser aplicados ao ambiente alguns ou todos os controles existentes na norma de segurança. A lista dos controles que devem ser aplicados depende de características do próprio ambiente, por exemplo, forma e local de armazenamento das informações, valor das informações armazenadas, quem poderá acessá-las, quais servidores estão instalados, quais tipos de serviços são disponibilizados aos usuários da rede interna e da rede externa, entre outros.

A Norma Nacional de Segurança de Informação (*NBR ISO/IEC 17799*) é dividida em 10 macros controles e cada um destes controles é subdividido em vários outros controles. Ao todo a *NBR ISO/IEC 17799* possui um total de 137 controles de segurança dos quais visam manter e gerir a segurança da informação nas empresas. Dessa forma, um estudo aprofundado da mesma é essencial nas organizações.

A seguir serão descritos alguns dos principais controles da Norma (*NBR ISO/IEC 17799).*

4.3 Principais controles da Norma (*NBR ISO/IEC 17799)*

4.3.1 Política de Segurança da Informação

Política de Segurança da Informação é um documento que descreve quais atividades os usuários estão autorizados a realizar, como e quando podem ser realizadas. É de vital importância que a alta administração apóie o uso da política e demonstre o seu comprometimento com a aplicação de suas penalidades cabíveis.

O objetivo da Política de Segurança da Informação é prover à direção uma orientação e apoio para a segurança da informação.

4.3.1.1 Documento da política de segurança da informação

É adequado que um documento da política seja aprovado pela direção e, além disso, publicado e comunicado para todos os funcionários da empresa. E é apropriado que este expresse as preocupações da direção com a gestão da segurança da informação, incluindo:

a) Declaração e comprometimento da alta direção, apoiando a análise da segurança da informação.
b) Referências à documentação que possam apoiar a política, por exemplo, políticas e procedimentos de segurança ou regras de segurança que os usuários devem seguir.

4.3.2 Segurança Organizacional

Segurança organizacional aborda a estrutura de uma gerência para a segurança de informação, assim como aborda o estabelecimento de responsabilidades incluindo terceiros e fornecedores de serviços.

O objetivo da segurança organizacional é gerenciar a segurança da informação na organização.

4.3.2.1 Infra-estrutura da segurança da informação

Uma infra-estrutura de gerenciamento de segurança da informação é necessária para iniciar e controlar a implementação da segurança da informação dentro da organização. Convém que um enfoque multidisciplinar na segurança da informação seja incentivado, tais como o envolvimento, cooperação e colaboração de gestores, usuários e administradores da empresa.

4.3.2.2 Atribuição das responsabilidades em segurança da informação

É adequado que as responsabilidades pela proteção de cada ativo e pelo cumprimento de processos de segurança sejam claramente definidas.

Também é necessário que a política de segurança da informação forneça um guia geral sobre a atribuição de regras e responsabilidades de segurança da informação na organização.

4.3.2.3 Cooperação entre organizações

Os contatos com organismos regulares, provedores de serviço de informação e operadoras de telecomunicações serão mantidos de forma a garantir que ações adequadas e apoio especializado possam ser rapidamente acionados na ocorrência de incidentes de segurança.

As trocas de informações de segurança serão restritas para garantir que as informações confidenciais da organização não sejam passadas para pessoas não autorizadas.

4.3.2.4 Segurança no acesso de prestadores de serviços

É importante que seja mantida a segurança dos recursos de processamento de informação e ativos organizacionais acessados por prestadores de serviço.

4.3.2.4.1 Tipos de acesso

O tipo de acesso dado a prestadores de serviço é de especial importância, tanto para acesso físico (escritórios, sala de computadores, gabinetes de cabeamento, etc) quanto acesso lógico (bancos de dados da organização, sistemas de informações, etc).

4.3.2.4.2 Contratados para serviços internos

Prestadores de serviços que mantém contrato devem permanecer dentro da organização por um período de tempo determinado, pois podem aumentar a fragilidade na segurança. Exemplos de prestadores de serviços.

a) Equipes de suporte e manutenção de software e hardware;
b) Alocação de estagiários e outras contratações temporárias;
c) Consultores.

É essencial entender as regras necessárias para administrar o acesso de prestadores de serviços e contratações temporárias. Convém que todas as regras de segurança resultantes do acesso de prestadores de serviços sejam colocadas nos contratos firmados.

O acesso por terceiros às instalações de processamento de informação da organização do mesmo modo deve ser controlado.

4.3.3 Classificação e Controle dos Ativos da Informação

A informação possui vários níveis de sensibilidade e criticidade, por isso é importante que ela seja classificada para indicar a importância, a prioridade e o nível de proteção.

O objetivo da classificação e do controle dos ativos da informação é assegurar que os ativos de informação recebam um nível adequado de proteção e manter a proteção adequada dos ativos da organização.

4.3.3.1 Contabilização dos ativos

Todos os princípios ativos da informação da organização devem ser inventariados e ter um proprietário responsável. O inventário de ativos ajuda a garantir que a proteção está sendo mantida de forma adequada. Os proprietários responsáveis pelos principais ativos deverão ser identificados e atribuídos da responsabilidade pela manutenção apropriada dos controles.

4.3.3.2 Inventário dos ativos

A informação dever ser classificada para indicar a importância, a prioridade e o nível de proteção. Um sistema de classificação da informação deve ser usado para definir um conjunto apropriado de níveis de proteção e determinar a necessidade de medidas especiais de

tratamento. É conveniente que cada ativo e seu respectivo proprietário sejam claramente identificados, e a classificação de segurança seja documentada. Exemplos de ativos:

a) ativos de informação: arquivos, informações armazenadas, documentação do sistema, manuais de usuário, procedimentos de recuperação, material de treinamento.
b) ativos de software: aplicativos, sistemas coorporativos, ferramentas (gráficas, desenvolvimento, tomada de decisão).
c) ativos físicos: fax, *no-breaks*, ar-condicionado, mídias magnéticas, monitores, *laptops*, roteadores.

4.3.4 Segurança em Pessoas

A segurança em pessoas envolve a seleção, a conscientização e as condições de trabalho de todos os funcionários, prestadores de serviço e usuários das instalações de processamento das informações, com o propósito de que eles estejam cientes e equipados para apoiar a política de segurança da organização durante a execução normal do seu trabalho.

O objetivo da segurança em pessoas é reduzir os riscos de erro humano, roubo, fraude ou uso de instalações não autorizadas.

4.3.4.1 Segurança na definição e nos recursos de trabalho

As responsabilidades de segurança devem ser atribuídas na fase de recrutamento dos funcionários, incluída em contratos e monitorada durante a vigência do contrato de funcionários. Usuários devem ser treinados nos procedimentos de segurança e no uso correto das instalações de processamento da informação, de forma a minimizar possíveis riscos de segurança.

4.3.4.2 Incluindo segurança nas responsabilidades do trabalho

Os incidentes que afetam a segurança devem ser notificados através dos canais apropriados o mais rápido possível. Todos os funcionários e prestadores de serviço devem estar conscientes dos procedimentos para notificação dos diversos tipos de incidentes que possam ter impactos na segurança dos ativos organizacionais.

4.3.4.3 Seleção e política de pessoal

É útil que regras sobre a equipe permanente sejam conduzidas no momento da seleção dos candidatos, contendo: a verificação das qualidades e conhecimentos apresentados no *curriculum vitae* e verificações acadêmicas e profissionais do candidato.

Em trabalhos que envolverem pessoas, é adequado que a organização verifique a idoneidade das mesmas, ou seja, tanto os indivíduos que tenham acessos às instalações de processamento da informação ou quanto àqueles que tratam de informações financeiras ou informações altamente confidenciais devem conter os atributos de confiança e credibilidade.

4.3.4.4 Termos de Trabalho

É apropriado que os termos e condições de trabalho determinem as responsabilidades dos funcionários pela segurança da informação.

4.3.4.5 Treinamento dos Usuários

É útil assegurar que os usuários estejam cientes das ameaças e das preocupações de segurança da informação na empresa. Além disso, é oportuno que eles sejam treinados nos procedimentos de segurança da informação e no uso correto das instalações de processamento de informações de forma a minimizar possíveis riscos de segurança.

4.3.4.6 Notificando o mau funcionamento de software

É adequado constituir procedimentos para mau funcionamento de software. Aconselha-se, por exemplo, que quaisquer mensagens apresentadas na tela sejam anotadas e que o assunto seja notificado imediatamente ao gestor de segurança da informação.

4.3.5 Segurança Física e do Ambiente

A segurança física e do ambiente é conveniente para assegurar os recursos e instalações de processamento de informações. Convém que a proteção fornecida seja proporcional aos riscos identificados.

O objetivo da segurança física e do ambiente é prevenir acesso não autorizado e dano às informações e instalações físicas da organização.

4.3.5.1 Áreas de Segurança

É de grande importância definir áreas de circulação restrita, e proteger equipamentos e a infra-estrutura de tecnologia da informação. Os recursos e instalações de processamento de informações, críticas ou sensíveis do negócio, devem ser mantidas em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas e controle de acesso.

4.3.5.2 Perímetro de Segurança

A proteção física pode ser alcançada através de diversas barreiras físicas na organização. Cada barreira estabelecerá um perímetro de segurança a acessos indevidos de pessoas não autorizadas dentro da organização. Indicam-se as seguintes diretrizes para que sejam avaliadas:

a) É útil que os perímetros de segurança sejam definidos;
b) As áreas restritas devem ter todas as portas externas protegidas, impedindo assim a entrada de pessoas não autorizadas, por exemplo, com o uso de alarmes e travas.

4.3.5.3 Segurança em salas e instalações de processamento

A seleção e o projeto de uma área de segurança deve levar em consideração as possibilidades de danos causados por desastres naturais ou causados pelo homem. Diante disso, é recomendado que os seguintes controles sejam analisados:

a) Instalações críticas devem ser localizadas de forma a evitar o acesso público;

b) Portas e janelas devem ser mantidas fechadas quando não utilizadas e instaladas proteções externas, sobretudo quando as mesmas se localizarem no térreo;

c) Instalações de processamento das informações internas devem ficar fisicamente separadas daquelas gerenciadas por prestadores de serviço;

d) Equipamentos de contingência e meios magnéticos de reserva (*backup*) devem ser guardados em uma distância segura da instalação principal.

4.3.5.4 Segurança dos equipamentos

Os equipamentos devem ser devidamente protegidos contra ameaças à sua segurança, perigos ambientais e principalmente dos acessos não autorizados.

4.3.5.5 Instalação e proteção de equipamentos

Os equipamentos devem ser instalados e protegidos para reduzir o risco de ameaças ambientais, perigos e acessos não autorizados. É indispensável adotar controles de forma a minimizar ameaças potenciais como roubo, fogo, explosivos, água, efeitos químicos, entre outros. E, além disso, é importante evitar o consumo de bebidas, alimentações e cigarros nas salas das instalações de processamento de segurança da informação.

4.3.6 Gerenciamento das Operações e Comunicações

Gerenciamento das operações e comunicações aborda as principais áreas que devem ser objetos de especial atenção da segurança. Dentre estas áreas destacam-se as questões relativas a procedimentos operacionais e respectivas responsabilidades, gerência de redes, controle e prevenção de vírus, controle de mudanças, execução e guarda de *back-up*, controle de documentação, segurança de correio eletrônico, entre outras.

O objetivo do gerenciamento das operações e comunicações é garantir a operação segura dos recursos de processamento da informação.

4.3.6.1 Procedimentos e responsabilidades operacionais

Os procedimentos e as responsabilidades pela gestão e operação de todos os recursos de processamento das informações devem ser definidos. Isto abrange o desenvolvimento de procedimentos operacionais e de resposta a incidentes.

4.3.6.1.1 Documentação dos procedimentos de operação

Procedimentos operacionais devem ser documentados e mantidos atualizados para futuras consultas, isto é, sempre que ocorra mudança nos sistemas e nos recursos de processamento da informação a documentação deverá ser consultada e atualizada.

4.3.6.2 Procedimentos para o gerenciamento de incidentes

As responsabilidades e gerenciamento de incidentes devem ser definidos para garantir uma resposta rápida e ordenada para os incidentes de segurança. Diante disso, recomenda-se que os seguintes controles sejam considerados:

a) Estabelecer procedimentos para cubrir todos os tipos de incidentes. Por exemplo: falha nos sistemas de informação e inoperância dos serviços;
b) Estabelecer procedimentos que contemplem a análise e a identificação das causas do incidente.
c) Relatar a ação tomada à autoridade apropriada.

4.3.6.3 Controles de rede

As redes de comunicações devem receber uma ampla atenção. As equipes técnicas devem implementar controles para garantir a segurança de dados e serviços disponibilizados contra serviços não autorizados, e procedimentos e responsabilidades devem ser estabelecidos para o gerenciamento de equipamentos remotos. Além disso, pode ser preciso a utilização de controles para proteção de dados sensíveis que transitam por redes públicas.

4.3.6.4 Descarte de mídias

As mídias devem ser descartadas de uma maneira segura quando não forem mais utilizadas, pois, informações sensíveis podem ser divulgadas ou utilizadas por pessoas de fora da organização através de mídias que não foram descartadas corretamente. As melhores técnicas para remoção de mídias são por meio de trituração e incineração. Os itens abaixo demandam descarte seguro:

a) papel carbono;
b) documento em papel;
c) relatórios impressos;
d) discos removíveis;
e) documentação de softwares.

4.3.6.5 Troca de informações e *software*

As trocas de informações e software entre organizações e as possíveis implicações nos negócios e na segurança relacionadas com o comércio eletrônico devem ser controladas com a finalidade de prevenir a perda, modificação ou mau uso de informações.

4.3.6.5.1 Segurança do comércio eletrônico

Todo controle de correio eletrônico da empresa é controlado por um servidor de e-mail, evitando que ataques ao correio eletrônico aconteçam. Existe uso de regras e criptografia para proteger a confidencialidade e integridade das mensagens eletrônicas, mensagens de marketing e publicidade (*spam*) até chegarem no usuário final.

4.3.7 Controle de Acesso

Este tópico aborda o controle de acesso a sistemas, a definição de competências, o sistema de monitoração de acesso e uso, a utilização de senhas, dentre outros assuntos.

Os acessos à informação e processo do negócio devem ser controlados na base dos requisitos de segurança e do negócio. Procedimentos formais devem ser estabelecidos para controlar a concessão às chaves de direitos de acesso aos sistemas de informação e serviços.

A cooperação dos usuários autorizados é essencial para a eficácia da segurança. Os usuários devem estar cientes de suas responsabilidades para a manutenção efetiva dos controles de acesso, considerando o uso de senhas e a segurança dos equipamentos de sua utilização.

O objetivo do controle de acesso é controlar o acesso às informações.

4.3.8 Desenvolvimento e manutenção de Sistemas

Os requisitos de segurança dos sistemas devem ser identificados e acordados antes do desenvolvimento dos sistemas de informação. Estes requisitos são: a infra-estrutura, as aplicações do negócio e as aplicações desenvolvidas pelo usuário. É adequado que o acesso aos sistemas de arquivos seja controlado.

O objetivo do desenvolvimento e da manutenção de sistemas é garantir que a segurança seja parte dos sistemas de informação.

4.3.9 Gestão da Continuidade do Negócio

Esta seção reforça a necessidade de se ter um plano de continuidade e contingência desenvolvido, implementado, testado e atualizado.

O processo de continuidade deve ser implementado para reduzir a interrupção causada por um desastre ou falha na segurança para um nível aceitável através de uma combinação de ações preventivas e de recuperação.

As conseqüências de desastres, falhas de segurança e perda de serviços devem ser analisadas. Os planos de contingência devem ser desenvolvidos e implementados para garantir que os processos do negócio possam ser recuperados no tempo devido.

O objetivo da gestão e da continuidade do negócio é não permitir interrupção das atividades do negócio.

4.3.10 Conformidade

A seção final aborda a necessidade de observar os requisitos legais, tais como a propriedade intelectual e a proteção das informações de clientes.

O projeto, a operação, o uso e a gestão de sistemas de informação podem estar sujeitos a requisitos de segurança contratuais, regulamentos ou estatutos.

Consultoria em requisitos legais específicos pode ser procurada em organizações de consultoria jurídica, ou em profissionais liberais, adequadamente qualificados nos aspectos legais.

O objetivo da conformidade é evitar violação de qualquer lei criminal ou civil, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança.

5 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

O crescente uso da internet, a disponibilização de novos serviços e linhas de negócios, e cada dia recursos de tecnologia da informação mais complexos, fazem da gestão de segurança da informação peça fundamental para qualquer empresa.

Nesse contexto, para que o gerenciamento seja efetivo e não dependa de talentos humanos, tornam-se necessárias à criação e a implementação de uma Política de Segurança da Informação, dirigida especialmente à organização e completamente integrada ao seu negócio.

A Política de Segurança da Informação é um conjunto de diretrizes, normas e procedimentos que devem ser seguidos e, além disso, visa conscientizar e orientar os funcionários, clientes, parceiros e fornecedores para o uso seguro do ambiente informatizado. Além disso, contém informações sobre como gerenciar, distribuir e proteger seus principais ativos.

Com uma Política de Segurança da Informação bem formatada, todos os processos da empresa ficam menos suscetíveis ao extravio de informações por responsáveis internos e externos, além de otimizar todos os processos e diminuir prejuízos por falhas ocasionais. A Política de Segurança da Informação é o ponto de partida para o gerenciamento dos riscos associados aos sistemas de informação ou aos processos da empresa, que conseqüentemente irá diminuir as vulnerabilidades que a empresa apresenta.

Para que uma Política de Segurança da Informação tenha sucesso dentro de uma empresa é importante que ela contemple algumas características das quais são essenciais a fim de que toda a energia empregada nesta tarefa seja bem aproveitada. Além disso, deve ter a participação de todos os funcionários da empresa.

A seguir são apresentadas as principais características de uma Política de Segurança da Informação:

- Usar uma linguagem simples, com poucos termos técnicos;
- Ser de fácil compreensão e aplicabilidade;
- Ser clara e concisa;
- Ter o apoio da alta direção;
- Estar de acordo com a realidade prática;
- Ser amplamente divulgada;
- Ser revisada periodicamente;
- Estar implementada.

5.1 Definição e Princípios da Política de Segurança da Informação

Para o cumprimento do que é estabelecido na Política de Segurança da Informação as atribuições e as responsabilidades devem ser bem definidas e estarem claras com os envolvidos. Dessa forma a empresa pode ser dividida em 5 grandes áreas para facilitar essas atribuições e responsabilidades. Abaixo será descrita cada uma destas cinco áreas que são: Comitê de Segurança da Informação, Proprietário das Informações, Área de Segurança da Informação, Usuários das Informações e Recursos Humanos, segundo Ferreira e Araújo:

Comitê de Segurança da Informação, Proprietário das Informações, Área de Segurança da Informação, Usuários das Informações e Recursos Humanos, segundo Ferreira e Araújo:

> Comitê de Segurança da Informação
>
> A função deste comitê deve ser de divulgar e estabelecer aos procedimentos de segurança, assim como se reunir periodicamente, ou a qualquer momento conforme requerido pelas circunstâncias, com o objetivo de manter a segurança em todas as áreas da organização.
> A reunião de gestores com visões do mesmo objeto, mas de pontos diferentes, é fundamental para a obtenção real dos problemas, desafios e conseqüências. Dessa forma, envolver representantes das áreas de

Tecnologia, Comercial, Jurídica, Negócio, Financeira, Auditoria, entre outras, trará muitos benefícios para a gestão da segurança da informação.
As responsabilidades do comitê incluem, mas não estão limitados a:

- Aprovação das políticas, normas e procedimentos de segurança da informação;
- Designação, definição ou alteração das responsabilidades da área de Segurança da Informação;
- Aprovação de novos controles ou alteração das responsabilidades da área de Segurança da Informação;
- Apoio à implantação de soluções para a minimização dos riscos;
- Suporte às iniciativas da área de Segurança da Informação;
- Deliberar sobre temas ou ações não definidos / incluídos em nenhuma norma já publicada.

O comitê deve ser composto por integrantes, com ou sem prazo fixo de mandato, nomeados pelo Conselho de Administração. As deliberações do comitê devem ser tomadas pela maioria dos membros que o compõe e a função de integrante do comitê ser indelegável.
Devem ser preparadas atas documentando o conteúdo das reuniões, que devem ser revisadas pelos integrantes do comitê e distribuídas ao demais participantes.
A política necessita especificar que, ao final dos semestres, ou em outro momento determinado pela organização, deve-se elaborar o documento denominado "Relatório do Comitê de Segurança" a ser enviado ao Conselho de Administração, contendo entre outros aspectos, as seguintes informações:

- Descrição das atividades exercidas durante o período;
- Avaliação da efetividade do sistema de controles de segurança, com ênfase nos regulamentos, códigos internos e cumprimento das leis em vigor;
- Análise dos resultados parciais e finais das ações de forma a medir efeitos, comparando-os às metas definidas e realizando os devidos ajustes;
- Descrição das deficiências detectadas, bem como das recomendações apresentadas à diretoria, com a indicação daquelas não acatadas e respectivas justificativas.

Proprietário das Informações

O proprietário das informações é o responsável pela autorização do acesso às informações, considerando as políticas vigentes dentro da organização. Suas responsabilidades e necessidades de conhecimento incluem, mas não estão limitadas a:

- Domínio sobre as informações geradas em sua área de negócio e atuação;
- Identificar e classificar as informações conforme critérios definidos pela política vigente na organização;
- Periodicamente revisar as informações classificadas;
- Garantir que os usuários entendam e sigam os procedimentos de segurança;
- Autorizar e revisar os acessos à informação.

Identificação dos proprietários

Com as classificações, regras e responsabilidades definidas, devemos identificar os proprietários das informações. Estes profissionais devem ser das unidades de negócio da organização, pois é ela que será afetada caso as informações tornem-se públicas ou sejam corrompidas / perdidas. Os seguintes critérios devem ser observados para a identificação deste responsável:

- Obrigatoriamente deve será a pessoa de negocio;
- O suporte dos altos executivos é um fator de sucesso;
- Para algumas funções de negócio, deve ser considerada a participação de mais de um executivo.

A identificação por etapas destes profissionais será mais bem conduzida ao invés de se tentar identificá-los todos de uma vez. A equipe formada e designada para desenvolver as regras e responsabilidades deve também desenvolver o plano inicial. Primeiramente, os dados críticos ou mais importantes para a organização devem ser identificados. É mais fácil identificar proprietários para esses tipos de informações. Outros proprietários poderão ser definidos posteriormente.

Área de segurança da informação

A função básica da Área de Segurança da Informação é proteger o ativo de informação, minimizando os riscos a níveis aceitáveis. Em algumas organizações, esta área também é responsável pela elaboração do plano de continuidade de negócio.
A implementação de controles por meio de processos para a proteção das informações é uma das formas de prover segurança aos sistemas de informação.
Suas responsabilidades incluem, mas não estão limitadas a:

- Fazer cumprir a Política de Segurança da Informação;
- Definir, implementar e revisar os controles;
- Identificar os riscos inerentes e residuais da segurança;
- Definir perfis e recursos para a realização das trilhas de auditoria;
- Definir os critérios e procedimentos para a realização da classificação da informação, protegendo as mais críticas;
- Avaliar os procedimentos de segurança reportando seus resultados e discutindo com os envolvidos as melhorias necessárias;
- Definir a estrutura de segurança a ser cumprida pelas áreas;
- Definir as soluções de segurança antes da implementação e durante a manutenção;
- Elaborar programas de treinamentos visando a capacitação dos proprietários e usuários da informação;
- Desenvolver, implementar e manter planos de continuidade que visem garantir as operações em casos de desastres e indisponibilidade dos sistemas de informação;
- Prover e administrar salvaguardas físicas contra acessos não autorizados, protegendo contra eventuais prejuízos no negócio;
- Monitorar o uso da *web* e do tráfego de mensagens de correio eletrônico.

Usuários das informações

> O usuário das informações é qualquer indivíduo com acesso às informações da organização, seja um funcionário ou um contratado, com atividades internas ou sem seu próprio escritório. Suas responsabilidades incluem, mas não estão limitadas a:
>
> - Entender e seguir a política assegurando que os procedimentos de segurança sejam respeitados e cumpridos;
> - Cumprir as regras de segurança determinadas pelas políticas vigentes na organização;
> - Utilizar as informações apenas para os propósitos do negócio;
> - Informar imediatamente ao canal de comunicação disponível qualquer violação / incidente de segurança.
>
> Recursos Humanos
>
> Esta área deve estabelecer as sanções e penalidades a serem aplicadas nas situações em que a política for desrespeitada.
> Também é responsabilidade do RH comunicar à área de Tecnologia da Informação, a ausência ou desligamento de funcionários. Deve haver m procedimento formal de comunicação, de forma que não exponha a organização a riscos desnecessários de uso não autorizado de contas de usuários ausentes.
> A área de Recursos Humanos deve auxiliar na obtenção da assinatura dos Termos de Responsabilidade de Segurança da Informação.
> Tal documento deve formalizar o conhecimento e a concordância do funcionário sobre as políticas estabelecidas para o uso adequado da informação e também das penalidades da organização e da lei. (FERREIRA E ARAÚJO,2006, pág 41 à 46)

A divisão da empresas em grandes áreas pode não ser aplicada em todos os tamanhos de empresas, pois principalmente em algumas empresas de pequeno porte, esta estrutura não é suportada pela empresa.

A seguir é apresentada uma fundamentação das operações da política de segurança da informação.

5.2 Fundamentação operacional da Política de Segurança da Informação

Neste item serão abordados os principais aspectos que devem ser contemplados no desenvolvimento de uma Política de Segurança da Informação, que são descritos a seguir.

5.2.1 Utilização dos recursos de TI

A utilização dos recursos de TI pelos colaboradores deve ocorrer apenas para o desenvolvimento de atividades diretamente relacionadas aos negócios da empresa. Deve ser definido nas políticas da empresa que os recursos tecnológicos não devem de maneira alguma ser utilizado para a prática de discriminação ou provocação em razão de sexo, raça, cor, religião, nacionalidade, idade, porte de deficiência, ou qualquer outra condição prevista em lei.

Os meios de comunicação da empresa não devem em hipótese alguma ser utilizados para receber, enviar ou armazenar conteúdos que sejam discriminatórios, difamatórios, participar de correntes (ver glossário) ou qualquer outro tipo de material que não estejam relacionados com os negócios da empresa.

5.2.2 Disponibilidade dos recursos de tecnologia da informação

A empresa deve somente disponibilizar recursos tecnológicos a colaboradores (funcionários ou terceiros) que estejam previamente autorizados pelos seus superiores, na finalidade de auxiliá-los no desempenho de suas funções e execução dos trabalhos.

Na Política de Segurança da Informação deve estar descrito que cada colaborador (funcionário) é responsável pela guarda, zelo e bom uso dos recursos que lhe foi concedido e caso isso não seja cumprido, implicará em medidas disciplinares.

5.2.3 Titularidade das informações

A Política de Segurança da Informação deve assegurar que todas as informações que são trocadas ou armazenadas em seus recursos de TI, independente de conteúdo são de propriedade única e exclusiva da empresa e que os colaboradores apenas utilizam os recursos disponibilizados pela empresa para a condução dos negócios da mesma. Deve ser estar bem claro que inclusive as mensagens de correio eletrônico são de propriedade única e exclusiva da empresa, ou seja, independente das que são trocadas com contatos particulares, familiares e afins.

A política também deve prever que podem ocorrer auditorias e que a empresa tem o direito de a qualquer momento acessar o conteúdo de qualquer usuário, independentemente do meio tecnológico que esteja armazenado. Por exemplo, em computadores, correio eletrônico, correio de voz, mídias ou até mesmo em materiais impressos.

Este tipo de ação deve ser suportado por um termo previamente assinado por cada usuário.

5.2.4 Segurança das informações

A responsabilidade pela segurança das informações deve estar estabelecida nos documentos oficiais da empresa e principalmente na Política de Segurança da Informação que cada colaborador da empresa é responsável pela segurança das informações dentro da empresa, principalmente pelas informações que estão sob sua responsabilidade.

Deve ser de conhecimento de todos a importância das senhas de acesso, ou seja, as mesmas não devem ser compartilhadas ou divulgadas para que outros colaboradores tenham acesso a informações confidencias ou que não lhes pertencem.

Para acesso a informações confidencias deve existir uma autorização formal por parte do diretor ou gerente responsável pela aprovação dos acessos, os quais têm o direito de acessar e garantir o sigilo das informações.

5.2.5 Autorização para uso dos recursos de tecnologia da informação

Uma política de liberação de acessos deve ser elaborada para descrever e formalizar quem são os responsáveis por liberar acessos a novos colaboradores ou liberar novos acessos a colaboradores já existentes. Esta política deve estabelecer que cada usuário deva somente e exclusivamente ter os acessos que possuem relação com suas tarefas. Uma hierarquia de responsabilidades como a que segue abaixo pode ser utilizada para facilitar o entendimento desta política:

> Diretor: poderá efetuar autorizações e aprovações necessárias para os diretores e gerentes sob sua subordinação direta;
> Gerente: poderá efetuar autorizações e aprovações necessárias para os gerentes, supervisores, encarregados e demais colaboradores sob sua subordinação direta.(FERREIRA E ARAÚJO, 2006, p.64).

5.2.6 Estações de trabalho e servidores

As estações de trabalho e os servidores merecem um acompanhamento no que diz respeito a sua utilização, pois devem ser apenas empregadas para a realização de atividades que estão diretamente relacionadas com as normas da empresa.

A seguir são apresentadas algumas considerações sobre segurança aplicadas às estações de trabalho:

- Precisam ser monitoradas para que usuários não instalem softwares que não são homologados pela empresa e que conseqüentemente a empresa não possui

licença sobre os mesmos. Devem ser bloqueados quaisquer tipos de jogos ou outros aplicativos que possam reduzir o desempenho dos usuários.

- Devem ser padronizadas de acordo com o que cada departamento ou colaborador necessita. Por exemplo, as estações que estão na produção não devem ter acessos aos sistemas de recursos humanos.
- Devem ser bloqueadas com uma senha quando os usuários ausentarem-se de seu local de trabalho. Pode ser a própria proteção do sistema operacional, proteção de tela com senha ou qualquer outro recurso oferecido pela empresa para esta finalidade. Este tipo de ação é importante para que usuários não autorizados venham a se privilegiar de acessos dos quais não possuem alvará.
- Devem conter controles sobre os dispositivos e *I/O* (entrada e saída) de informações na empresa, como: *drives* de disquete, gravadores de CDs, gravadores de *Dvds*, dispositivos *UBS* e quaisquer outros meios físicos que permitam a entrada e principalmente a saída de informações sem controle. A saída ou utilização destes recursos deve ser autorizada formalmente.
- Devem ter dispositivos extras de segurança que não permitam o acesso não autorizado às informações que estão contidas nele, Neste caso, aplicado às Estações de trabalho móveis (*notebooks/laptops*).
- Os servidores devem ter o acesso físico restrito e sua utilização deve ser apenas para suas aplicações principais. Por exemplo, um servidor não deve ser usado para ficar navegando na internet.

5.2.7 Proteção contra softwares maliciosos ou não autorizados

Os vírus de computador são apontados como o principal problema de segurança da informação atualmente.

A principal e mais utilizada forma de proteção contra os vírus são os chamados antivírus, ou seja, softwares que são desenvolvidos baseados em regras que detectam a presença de códigos maliciosos que estejam presentes na máquina.

Como a evolução dos vírus é muito rápida o antivírus utiliza-se de atualizações para o seu software para que o mesmo fique conhecendo os novos vírus, bem como formas de combatê-los. As atualizações para este tipo de software são praticamente diárias.

Todos os computadores da empresa devem possuir um antivírus instalado e programado para que seja atualizado constantemente, e de preferência, que não dependa de uma ação do usuário. O antivírus deve estar configurado para verificar todos os arquivos que são enviados e principalmente recebidos através do correio eletrônico.

As políticas da empresa devem ser claras ao ressaltar a usuários que todos os softwares utilizados na empresa possuem licença de uso e são homologados, e que não é permitida a instalação de qualquer software sem autorização formal da área de TI.

> Uma publicação americana observou que "usuários sempre são usuários". Ainda que a organização ofereça uma máquina rápida, repleta de memória, certamente ele tentará instalar seus próprios programas. E, por isso, impedir que usuários acrescentem softwares não autorizados em seus computadores de mesa ou *notebooks* se tornou uma preocupação comum entre os gerentes de TI. (FERREIRA E ARAÚJO, 2006, p. 67).

5.2.8 Procedimentos para acesso à Internet

Atualmente a internet é um dos principais meios de comunicação utilizada para pesquisas, consultas bancárias, informações sobre atualidades, enfim é praticamente indispensável no local de trabalho. Mas embora seja uma poderosa ferramenta para os colaboradores, a internet pode vir a ser uma grande vilã quando se trata de produtividade, pois

estudos revelam que o acesso em banda larga pode levar um usuário a desperdiçar até 20 % do seu tempo produtivo acessando conteúdos para fins particulares.

A utilização da internet deve ser baseada em um procedimento que vise padronizar o uso da mesma, com a finalidade de proteger a propriedade intelectual, privacidade das informações e quaisquer tipos de discriminação.

É importante que neste procedimento seja explanado a importância da internet para a condução dos negócios da empresa, de modo que fiquem esclarecidos aos usuários os principais processos que podem causar danos quando são utilizados de maneira inadequada. Por exemplo, uma filial da empresa utiliza a internet para conectar no sistema de gestão para lançar os seus pedidos de venda.

As páginas da internet são das mais variadas formas e podem trazer tanto conteúdos úteis, como conteúdos maliciosos que possa danificar o computador ou até mesmo a rede que está lhe acessando. É muito comum que os *sites* utilizem *cookies* (ver glossário), para conhecer o perfil de cada usuário.

A integridade e transparência do nome da empresa podem vir a ser abalada pelo uso indevido da internet por parte dos seus colaboradores, pois praticamente tudo que é feito na internet é monitorado e armazenado e a prática de atividades ilegais pode ser identificada por intermédio de técnicas que conseguem identificar os dados como *IP*, data e hora da conexão, afinal tudo isso poderá acarretar sérios problemas para a empresa.

A monitoração do uso da internet é muito importante para que sejam registrados todos os acessos de cada usuário e os mesmos possam ser notificados e até mesmo punidos nos casos de acesso que sejam contrários a política da empresa. Para fins de auditoria e comprovação dos acessos é indispensável que algumas informações sejam armazenadas juntamente com os *sites* utilizados. Alguns dos principais dados que precisam ser

armazenados são: identidade do usuário, data e hora da conexão, endereço *IP* de origem, protocolos utilizados e quantidade de dados sendo transmitidos e/ou recebidos.

Quanto à abrangência dos procedimentos de utilização dos recursos da internet é importante que os mesmos sejam analisados pelo Departamento Jurídico da empresa. Devem ser contemplados os seguintes aspectos:

- Se os funcionários terão permissão para navegar na *Web* para uso pessoal e / ou fins comerciais;
- Se os funcionários poderão usar a Internet para fins particulares e em quais períodos (durante o almoço, depois do expediente, etc.);
- Se e como a organização efetuará a monitoração do uso da Internet e a qual nível de privacidade os funcionários estão sujeitos;
- Acessos não permitidos, determinando os tipos de *sites* que serão inaceitáveis, como:

> *Download* de conteúdo ofensivo ou preconceituoso;
> Atitude ameaçadora ou violenta;
> Atividades ilegais;
> Solicitações comerciais (não relacionadas ao trabalho);
> Outros aspectos que a organização julgar necessários. (FERREIRA E ARAÚJO, 2006, p. 69).

Neste procedimento também devem constar as sanções para os tipos de acesso que forem julgadas inadequadas pela empresa.

Todos os usuários devem receber um treinamento sobre este procedimento, bem como instruções para uma navegação segura e assinar termos de ciência deste procedimento.

5.2.9 Procedimentos para uso de correio eletrônico

A utilização do correio eletrônico no meio corporativo é uma prática cada vez mais adotada pelas empresas para trocarem informações de uma maneira rápida e prática, e também como garantia de documentação.

Quando o assunto é segurança da informação o uso do correio eletrônico oferece diversos riscos para a empresa. Recentemente têm surgido diversas maneiras de burlar o correio eletrônico e utilizá-lo para a propagação de vírus, acesso não autorizado a mensagens e envio de *spams* (ver glossário).

E apesar dessas várias maneiras de fraudar as mensagens do correio eletrônico, não se pode desconsiderar que ele pode ser utilizado por funcionários mal intencionados para enviar informações confidenciais sem a autorização dos responsáveis, provocando impactos inesperados às empresas.

Dessa forma, a política de segurança da informação deve tratar a questão do correio eletrônico com bastante cautela, para que pontos importantes na utilização deste recurso sejam tratados conforme as necessidades da empresa e que sigam os preceitos de segurança. Além disso, a elaboração desta parte da política deve ser analisada e aprovada pelo Departamento Jurídico da empresa, para que sejam avaliadas as normas legais para evitar a invasão de privacidade de cada usuário e não deixar a mesma vulnerável.

5.2.10 Gerenciamento, controle da rede, monitoração do uso e acesso aos sistemas

As políticas de controle de acesso devem abranger os recursos tecnológicos que pretendem proteger e a quem se devem dar privilégios e acessos. A proteção está baseada no que cada usuário pode ou não pode acessar em determinados sistemas, que em sua grande maioria é realizada por intermédio de um ID e senha durante o processo de *logon.*

> Os controles de acesso lógico devem assegurar que:
>
> - Apenas os usuários autorizados tenham acesso aos recursos;
> - Os usuários tenham acesso apenas aos recursos realmente necessários para a execução de suas atividades.
> - O acesso aos recursos críticos seja constantemente monitorado e restrito;
> - Os usuários sejam impedidos de executar transações incompatíveis com a sua função.
>
> Controle de acesso pode ser resumido nas funções:
>
> - Identificação e autenticação de usuários;
> - Gerenciamento e monitoramento de privilégios;
> - Limitação e desabilitação de acessos e na prevenção de acessos não autorizados.
>
> O processo adequado para a manutenção de um controle efetivo sobre os acessos aos sistemas requer processos com intervalos periódicos para a revisão das contas de usuários e seus respectivos privilégios. Dessa forma, a organização deve padronizar os seguintes aspectos:
>
> - Todas as solicitações de acesso devem ser formais e devidamente aprovadas pelos níveis requeridos;
> - Os acessos de usuários devem ser revistos periodicamente e sempre que houver alguma alteração no ambiente dos sistemas, incluindo também administradores ou quaisquer outros tipos de acesso privilegiado;
> - Os usuários que forem demitidos devem ser removidos de forma imediata dos sistemas;
> - As contas dos usuários afastados ou em férias devem ser bloqueadas temporariamente;
> - A comunicação dessas situações deve ocorrer por meio de procedimento efetuado pelo departamento pessoal ou de recursos humanos. A periodicidade da comunicação deve ser mensal para os casos de afastamento e férias, no entanto, para os casos de demissão, a mesma deve ser imediata. (FERREIRA E ARAÚJO, 2006, p. 71 à 72).

Os controles e processos acima citados são primícias para que os pilares da segurança da informação sejam mantidos dentro da empresa, pois a falta destes controles coloca em risco a integridade, confidencialidade e disponibilidade das informações.

5.2.11 Identificação e autenticação do usuário

A identificação do usuário, ou *User ID*, deve ser único, ou seja, cada usuário autorizado deve possuir o seu. Deve ser evitado de todas as formas a utilização de usuários e senhas compartilhadas.

É por intermédio do *ID* de cada usuário que é possível rastrear o que foi realizado por determinado usuário nos sistemas. Dessa forma, é possível identificar de maneira segura quem foi o usuário responsável por determinada ação nos sistemas da empresa.

5.2.12 Senhas

A criação de senhas merece também uma atenção especial na Política de Segurança da Informação. É importante que a Política defina claramente algumas regras para a criação de senhas.

A Política de Segurança da Informação pode trazer exemplos de como não criar uma senha, tais como: números seqüenciais, datas de nascimento, sobrenome, placa de carros, entre outros, pois esses dados são muito fáceis de se obter e qualquer pessoa poderia utilizar esse tipo de informação para uma autenticação válida.

Os sistemas devem ser configurados para não permitir a criação de senhas consideradas de fácil descobrimento e devem ter alguns parâmetros básicos para ajudar neste trabalho. A seguir alguns destes parâmetros são apresentados:

- Número de caracteres para composição da senha: deve ser composta no mínimo por seis caracteres;
- Expiração da senha: deve ser forçada a alteração das senhas dos usuários periodicamente;
- Repetição de senha: restringir, pelo menos, a utilização das últimas cinco senhas utilizadas;
- Quantidade de tentativas inválidas de acesso: deve haver um limite para realizar o bloqueio das tentativas de acesso inválidas, de forma a evitar a descoberta das senhas. A boa prática sugere três tentativas;

- Troca de senhas iniciais (*default*): As senhas iniciais dos sistemas, banco de dados e quaisquer outros produtos, devem ser trocadas de forma imediata, antes de sua utilização em ambiente seguro;
- Bloqueio automático por tempo de inatividade (*Time Out*): Os sistemas devem possuir tempo máximo determinado para realizar bloqueio/término de um acesso por inatividade.

5.2.13 Cópias de Segurança e Recuperação das informações

A disponibilidade das informações é um dos pilares da segurança da informação, sendo fundamental para qualquer organização, independentemente de seu tamanho, possuam um procedimento de cópias de segurança (*backup*) e recuperação (*restore*) de informações, os quais sejam capazes de orientar as ações de realização e recuperação das informações.

A Política de Segurança deve fornecer as diretrizes necessárias para orientar o desenvolvimento dos procedimentos de cópias de segurança e recuperação das informações. O valor da informação produzida na organização, além do valor estratégico, é também a soma de inúmeras horas de trabalho no desenvolvimento de documentos, informações, produtos, entre outros esforços que provavelmente em qualquer tentativa de quantificar seu valor, será encontrado um número aproximado, porém dificilmente exato e com grandes probabilidades de que para cada cálculo realizado tenha um valor diferente.

Para a implementação da cópia de segurança deve-se levar em consideração a importância da informação, o nível de classificação utilizado, sua periodicidade de atualização e também sua volatilidade. Com base nos conceitos apresentados, a empresa deve ter as seguintes premissas nos seus procedimentos de *backup*:

- Realizar *backup* visando diminuir os riscos de continuidade;

- Manter os *backups* em local físico distante da localidade de armazenamento dos dados originais;
- Realizar testes nas mídias que armazenam os *backups* para assegurar que os mantidos em ambiente interno e externo estejam seguros e em perfeito estado para serem utilizados;
- Desenvolver e manter a documentação dos procedimentos de *backup* e *restore* sempre atualizada;
- Assegurar que seja mantido um inventário sobre as mídias que armazenam os *backups*.

A freqüência para a realização dos *backups* e as respectivas retenções deve ser determinada considerando a velocidade e a volatilidade da informação, ou seja, depende da periodicidade em que os dados são alterados.

A Política de Segurança da informação também deve apresentar a maneira de como os testes de restauração devem ser realizados e qual a periodicidade para os mesmos, com a finalidade de:

- Verificar a integridade da informação armazenada;
- Avaliar a funcionalidade dos procedimentos;
- Identificar procedimentos desatualizados ou ineficazes;
- Identificar falhas ou defeitos.

5.2.14 Controle de acesso físico às áreas sensíveis

A segurança em tecnologia da informação pode ser compreendida por dois principais aspectos: segurança lógica e segurança física. A segurança física desempenha um papel tão

importante quanto a segurança lógica, pois elas são a base para a proteção de qualquer investimento feito por uma empresa.

Qualquer acesso às dependências da empresa, desde as áreas de trabalho até aquelas consideradas críticas, deve ser controlado e sempre praticando sua formalização.

Os sistemas de segurança física devem ser implementados para garantir que somente terão acesso aos locais seguros da empresa as pessoas que tiverem autorização e permissão formal.

5.2.15 Segurança e tratamento de mídias

Para as informações contidas em computadores, discos e outros equipamentos que serão descartados ou transferidos para outros usos, devem-se assegurar que estas estarão definitivamente destruídas, sem risco de comprometer a perda de confidencialidade.

Com isso, todos os recursos capazes de armazenar informações devem ser definidos como mídias e a organização deve possuir procedimentos específicos para orientar todo o tratamento das mesmas.

Depois de terem sido julgados os principais aspectos que uma Política de Segurança da Informação deve abordar, imediatamente cabe à empresa avaliar quais são aplicáveis e redigir os procedimentos para cada um deles, compondo assim a Política de Segurança da Informação da empresa.

5.3 Principais benefícios alcançados

Se a política implantada for efetiva, ou seja, se ela apresentar as características necessárias como: simplicidade, comprometimento de todos os envolvidas da organização,

exatidão, e estar adequada para todos, certamente ela obterá alguns benefícios. De acordo com Ferreira e Araújo (2006) os principais benefícios são classificados de acordo com o prazo, dos quais são:

Curto prazo

- Formalização e documentação dos procedimentos de segurança seguidos pela empresa.
- Implementação de novos procedimentos e controles
- Precaução de acessos não autorizados, danos ou interferências do fluxo dos negócios.
- Maior segurança nos processos de negócio.

Médio prazo

- Padronização das metodologias de segurança incorporados na rotina da empresa.
- Adequação segura de novos processos do negócio.
- Qualificação dos sistemas de respostas a incidentes.
- Conformidade com a Norma ISO/IEC 17799.

Longo prazo

- Retorno do investimento aplicado, por meio da redução de incidentes decorrentes por problemas relacionados à segurança.
- Solidificação da imagem associada a Segurança da Informação.

A seguir será apresentado um estudo de caso, mostrando a atual situação da empresa, e em seguida serão apontadas algumas soluções com base nas deficiências encontradas com relação à segurança da informação.

6 ESTUDO DE CASO

6.1 Apresentação da empresa e metodologia

O estudo de caso foi realizado em uma indústria do ramo alimentício/farmacêutico e que está localizada na região centro-oeste do Estado de São Paulo. A SAF (nome fictício dado à empresa para preservar sua integridade) é uma empresa que está há mais de 45 anos no mercado e é uma das empresas de destaque no seu segmento, contando atualmente com aproximadamente 200 funcionários.

A parceria com a empresa SAF foi viabilizada devido um dos integrantes do grupo deste TCC (Trabalho de Conclusão de Curso) conhecer o Gestor do Departamento de Tecnologia da Informação da empresa, o qual já havia exposto a necessidade de um estudo sobre Segurança da Informação na empresa.

Como a empresa SAF tinha a necessidade de realizar um estudo sobre Segurança da Informação foram realizadas duas reuniões entre os integrantes do grupo e o Gestor do Departamento de Tecnologia da Informação para que fossem identificadas as necessidades da empresa com relação a Segurança da Informação.

A empresa SAF apresentou para o grupo deste TCC que suas principais necessidades atualmente para Segurança da Informação são: um estudo sobre os principais problemas que a empresa apresenta atualmente e como estes problemas podem ser solucionados sem que a SAF tenha que realizar grandes investimentos em ferramentas e tecnologias de Segurança da Informação. O objetivo da empresa SAF é utilizar-se deste estudo como base para o início de suas ações para aumentar e melhorar sua Segurança das Informações.

A empresa SAF gentilmente permitiu a permanência dos alunos durante vários dias acompanhando o cotidiano de trabalho da mesma e, além disso, permitiu que diversos

funcionários fossem entrevistados, inclusive o Presidente e os Diretores da Empresa, mostrando o comprometimento da alta direção para com o assunto.

Para que fosse possível a identificação dos principais problemas de Segurança da Informação que a SAF apresenta atualmente foi realizado um acompanhamento dos trabalhos realizados pelos seus funcionários. Este acompanhamento foi o primeiro passo para que fosse possível conhecer como é o dia a dia dos funcionários da Empresa e qual a importância que é dada por eles para a Segurança das Informações da Empresa.

Baseado no que foi encontrado no dia a dia de trabalho da empresa em conjunto com seus atuais objetivos para Segurança da Informação foram elaboradas entrevistas direcionadas aos seguintes departamentos da Empresa: Presidência, Diretorias, Tecnologia da Informação, Recursos Humanos, Administrativo / Financeiro, Industrial, Pesquisa & Desenvolvimento e Garantia da Qualidade / Controle da Qualidade. Cada questionário de entrevista (ver apêndices) constituiu-se de questões das quais eram diretamente ligadas ao departamento em estudo, para que facilitasse a análise de cada item internamente no departamento, o que conseqüentemente iria refletir para a Empresa como um todo, após a consolidação das entrevistas.

Para a elaboração das questões em cada uma das entrevistas foram considerados como bases os conceitos apresentados nos capítulos anteriores, principalmente o terceiro e o quinto capítulo, no entanto, alguns tópicos destes capítulos não foram abordados na elaboração das questões e na continuidade do estudo na Empresa por terem sido classificados como não aplicáveis para o momento.

O método de entrevista foi o escolhido para o levantamento por oferecer a possibilidade de questionamentos durante a entrevista, dando a oportunidade dos entrevistadores conseguirem absorver o máximo de cada entrevista.

Em seguida, com base em tudo o que foi identificado na empresa, ou seja, com o apoio das entrevistas realizadas com os diversos funcionários da empresa e com o devido acompanhamento diário dos funcionários, foi possível fazer um panorama com a atual situação da empresa com relação à Segurança das Informações.

A seguir será apresentado o panorama atual da empresa para cada tópico avaliado, bem como as soluções propostas para cada tópico.

6.2 Panorama atual da empresa e Soluções Propostas

6.2.1 Política de Segurança da Informação

Existe atualmente uma Política que define algumas regras e as boas práticas para o uso dos recursos computacionais e de telecomunicações. Esta Política é chamada de Política de Utilização dos Recursos Computacionais e de Telecomunicações. Em boa parte ela contempla os requisitos para uma Política de Segurança da Informação, porém não aborda os tópicos com a ênfase e detalhamento que receberiam se fizesse parte de uma Política de Segurança da Informação.

Este documento foi publicado na empresa no ano de 2003 e até hoje não sofreu nenhuma revisão. Foi verificado que o mesmo não apresentou uma correta divulgação pela empresa, pois muitos dos entrevistados não conseguiram se recordar como tiveram ciência deste documento e os que conseguiram lembrar entraram em divergência com o que foi apresentado pelo Departamento de Tecnologia da Informação, que foi o responsável pela elaboração e divulgação da política.

Segundo o Departamento de Tecnologia da Informação, a divulgação do documento ocorreu por intermédio de uma reunião com todos os gestores das áreas, na qual ficou

definido que cada gestor era responsável pela divulgação dentro de suas áreas de responsabilidades.

Soluções propostas:

- Revisar a Política atual, pois já se passaram três anos de sua implantação, sem nenhuma revisão;
- Criar um Comitê de Segurança da Informação, para que possa ajudar na revisão da Política atual;
- Realizar um treinamento com todos os colaboradores da empresa após a revisão deste documento;
- Ministrar o treinamento por um pessoal que tenha amplo conhecimento do assunto, para evitar eventuais dúvidas;
- Formalizar que todos têm ciência do que a Política de Segurança da informação rege, para evitar problemas futuros.

6.2.2 Titularidade das Informações

A Política atual da empresa fala sobre a titularidade das informações, ela define que a empresa tem todos os direitos sobre toda e qualquer informação que esteja armazenada nos recursos tecnológicos da empresa e que é propriedade da empresa. No entanto, foi constatado que isto não está muito claro para todos os usuários, o que pode trazer sérios problemas para a empresa caso seja necessário tomar alguma atitude embasada nesta política.

Soluções propostas:

- Com a devida divulgação da nova Política, conforme citado no item anterior este problema será solucionado, uma vez que a Política abrange este tema.

6.2.3 Segurança das Informações

A Segurança das Informações foi apresentada por praticamente todos os departamentos como uma questão de fundamental importância para a empresa. A Política existente estabelece alguns pontos sobre Segurança das Informações, e quem são os responsáveis diretos e indiretos.

A Segurança das Informações na SAF apresentou diversas falhas e vulnerabilidades da empresa em diversos aspectos e setores da mesma.

Algumas das principais falhas encontradas foram:

- Falta de controle efetivo de pessoas que entram e saem da empresa com câmeras digitais, celulares com câmera, *pen drivers*, disquetes e outros dispositivos de armazenamento;
- Falta de identificação dos gestores de ativos, principalmente em ativos do tipo informação;
- Ausência de um treinamento sobre a importância do ID's e senhas dos usuários, principalmente com funcionários mais antigos da empresa, que ingressaram antes de 2005;
- Não existe controle sobre envio e recebimento de mensagens pelo correio eletrônico, todos que têm acesso a esta ferramenta podem enviar e receber anexos;
- Praticamente todas as estações de trabalho possuem unidades de disquete e USB liberados;
- Insuficiência de controle sobre a impressão de ordens de produção, pois as mesmas trazem as fórmulas dos produtos na íntegra;

- Falta de cuidado com a impressão e manuseio de documentos contendo informações estratégicas e confidenciais, que são deixados próximos às impressoras por horas e até mesmo por dias.

Soluções propostas:

- Realizar um controle efetivo de pessoas que entram na empresa com dispositivos como: câmeras, celulares com câmera, filmadoras e afins, inclusive a entrada de funcionários com este tipo de equipamento;
- Melhorar a identificação dos gestores dos ativos da empresa;
- Fortalecer no treinamento da nova Política a importância do ID e senha de cada usuário;
- Adquirir um sistema que consiga controlar o envio / recebimento de mensagens de correio eletrônico, principalmente que consiga dividir os usuários em grupos com diferentes tipos de acesso a este recurso, como por exemplo: os que podem e os que não podem enviar ou receber mensagens com anexos;
- Remover das estações de trabalho as unidades de disquete, CD Rom e bloquear as portas do tipo USB;
- Criar um mecanismo que controle a impressão de ordens de produção e outros documentos que possuam informações altamente confidenciais, como as fórmulas que estão nas ordens de produção.

6.2.4 Classificação das Informações

Não existe a classificação das informações na SAF, ou seja, elas são classificadas quanto a sua sensibilidade ou importância para a empresa. O que foi considerado por muitos com relação à classificação das informações é o fato de terem uma área da rede de arquivos

em que é possível determinar níveis de acessos diferentes para usuários distintos. Esta área da rede mencionada pelos usuários é considerada pelo Depto. de TI como sendo uma importante área de armazenamento de informações, sejam elas confidenciais ou não, porém a falta da classificação destas informações não permite que seja realizado um trabalho efetivo para a proteção de uma maneira mais intensa nas informações classificadas como críticas e confidenciais.

Soluções propostas:

- Iniciar um trabalho de classificação das informações, pois atualmente isso não existe na empresa, ou seja, identificar junto aos gestores em qual nível de classificação (internas, públicas ou confidenciais) cada grupo de informações pertence, para que seja aplicado o nível de segurança adequado para cada nível de classificação.

6.6 Sigilo das Informações

Como não existe uma classificação das informações é difícil para a SAF poder controlar e garantir o sigilo das informações. Foi apurado que informações consideradas confidenciais pelos departamentos são enviadas pelo correio eletrônico sem nenhum controle, isto é, qualquer indivíduo que tenha acesso à informação pode a qualquer momento enviar um arquivo anexado em uma mensagem de correio eletrônico sem o controle ou autorização de um superior.

Do mesmo modo, não há na empresa uma política de mesas e telas vazias, com o intuito de diminuir a oportunidade de pessoas não autorizadas obterem acesso a informações confidenciais ou sigilosas da empresa.

Soluções propostas:

- Após o trabalho de classificação das informações será possível controlar de uma maneira efetiva as informações sigilosas;
- No treinamento da nova Política falar sobre a importância de não deixar informações importantes espalhadas pela mesa;
- Destacar também no treinamento a importância de bloquear a estação de trabalho quando se ausentar.

6.2.6 Autorização para acesso a recursos tecnológicos

A autorização para novos acessos e novos usuários está bem definida na Política atual da empresa, e este foi um ponto no qual observou-se que praticamente todos apresentam ciência da hierarquia existente e seguem a regra estabelecida na Política vigente. Um ponto fraco encontrado foi que uma simples mensagem de correio eletrônico ou do sistema de comunicação interna da empresa, enviada pelas pessoas autorizadas já é suficiente para a liberação do acesso.

Soluções propostas:

- Criar um mecanismo um pouco mais formal para a solicitação. Por exemplo, um documento específico para a solicitação de novos usuários ou novos acessos, que force o solicitante a refletir principalmente o motivo pelo qual está fazendo esta solicitação e se realmente é necessário para o momento.

6.2.7 Proteção contra vírus e softwares maliciosos

Todas as estações de trabalho possuem sistema de antivírus instalados e os mesmos são atualizados diariamente. A atualização não é totalmente automatizada, pois depende da confirmação do usuário para aceitar ou não que o arquivo de atualização seja executado na estação de trabalho.

Os usuários em sua grande maioria não receberam nenhum tipo de treinamento com relação ao uso deste tipo de software de maneira adequada, possibilitando assim o acesso a arquivos que possam estar infectados sem uma verificação anterior.

A Política estabelece também que a empresa reserva-se no direito de recusar determinados tipos de arquivos ou conteúdos, principalmente pelo correio eletrônico, esta prática não está muito bem difundida pelos usuários, pois eles não sabem exatamente quais os tipos de arquivos que são recusados pela empresa e também não possuem a adequada instrução de leitura para as mensagens de correio eletrônico o qual o servidor gera automaticamente quando acontece este tipo de situação.

Soluções propostas:

- Implantação de um sistema de antivírus do tipo corporativo, o qual oferece mais recursos e maior controle das estações de trabalho;
- Deixar claro na nova Política como é estabelecida a recusa de determinados tipos de arquivos, e quais são estes tipos;
- Implantar um sistema de anti *spam*.

6.2.8 Procedimentos para acesso a internet

A Política existente define que o acesso à internet pelos usuários é previamente autorizado pelos seus superiores. O acesso acontece após a validação de usuário e senha. Existe um *firewall* que faz um controle de conteúdo e monitora todos os acessos de todos os

usuários. Praticamente, todos têm ciência de que os acessos realizados na internet são arquivados para fins de auditoria por parte do gestor responsável pela área.

Por outro lado, os gestores não têm total ciência de que podem a qualquer momento solicitar relatórios dos acessos dos usuários que estão sob sua responsabilidade.

Soluções propostas:

- Implementar uma ferramenta que gerencie melhor os acessos dos usuários e que consiga fornecer relatórios de uma maneira prática;
- Controlar os usuários de ferramentas de mensagem instantânea, inclusive a lista de contatos de cada um, para evitar desperdício de tempo;
- Enviar relatórios periódicos para os gestores.

6.2.9 Procedimentos para Correio Eletrônico

A Política existente aborda o tema de correio eletrônico, definindo claramente como é liberado o acesso a este recurso, e como se deve utilizar tal ferramenta. Ao mesmo tempo, na Política se determinam boas práticas de utilização do e-mail corporativo.

Uma grande falha que a utilização desta ferramenta apresenta é que não existe um controle efetivo sobre o envio / recebimento de e-mails, principalmente com anexos, apenas são bloqueados alguns tipos de extensões de arquivos (*.exe*, *.bat*, *rom*, por exemplo), todavia todos os usuários de correio eletrônico podem enviar anexos (*.doc*, *.pdf*, *.ppt, por exemplo).* Esta é uma grande falha, pois arquivos confidenciais podem sair da empresa sem o conhecimento dos responsáveis pela informação.

Soluções propostas:

- Adquirir ou desenvolver um sistema que seja capaz de controlar o envio/recebimento de mensagens com anexos e dividir os usuários em grupos,

por exemplo, usuários que podem apenas enviar mensagens com anexo internamente, definir conforme a necessidade atual.

6.2.10 Gerenciamento, controle da rede, monitoração do uso e acesso aos Sistemas

Na Política de Segurança da Informação, o gerenciamento e controle dos acessos aos sistemas, rede e demais recursos que necessitam de um ID e senha, está definido que para a solicitação destes recursos é necessário que se faça uma solicitação formal do Supervisor ou Gerente para o Depto. de TI, mencionando o usuário e quais os acessos ele obterá.

A hierarquia definida nesta Política é respeitada e utilizada na prática.

Somente um problema foi observado neste tópico, com relação a usuários afastados ou de férias, ou seja, quando os mesmos estão ausentes da empresa por algum dos motivos citados, eles não têm suas contas bloqueadas nestes períodos, o que pode facilitar para que pessoas não autorizadas venham a utilizar o *login* destes usuários, perdendo a rastreabilidade do que efetivamente cada usuário fez com seu *login.*

Soluções propostas:

- Acrescentar na política que usuários que saem de férias, licença médica ou por qualquer outro motivo se afastem do trabalho por um período determinado, devem ter seus usuários bloqueados neste período.

6.2.11 Senhas e processo de *logon*

A Política existente aborda os aspectos de senhas e processos de *logon* e trata aspectos como número mínimo de caracteres e quantidade de conexões simultâneas.

Na prática não são utilizados todos os conceitos apresentados na Política, alguns dos principais problemas encontrados foram:

- Senhas genéricas;
- Senhas sem o tamanho mínimo;
- Sistemas não configurados para rejeitar senhas anteriores;
- Senhas não expiram depois de determinado período;
- *Login* não é bloqueado depois de um grande tempo de inatividade.

Soluções propostas:

- Não permitir o uso de usuários genéricos;
- Configurar os sistemas operacionais e demais softwares utilizados pela empresa para não permitirem a criação/alteração de senhas que não cumpram com o comprimento mínimo estipulado pela política;
- Configurar os sistemas operacionais e demais softwares utilizados pela empresa para não permitirem o uso das últimas senhas de cada usuário;
- Configurar os sistemas para bloquearem automaticamente no caso de ser digitado a senha errada um determinado número de vezes, conforme definido na política;
- Configurar os sistemas para bloquearem a estação de trabalho automaticamente caso haja um determinado período de inatividade, conforme estabelecido pela política.

6.2.12 *Backup* e Plano de contingência

A Política atual da empresa aborda aspectos de *backup*. Foi verificado que são realizados *backups* diários e mensais de parte dos servidores, porém alguns servidores ou

equipamentos que possuem informações críticas não possuem *backup*, devido a falta de espaço nas mídias de armazenamento de *backup.*

O sistema para realização de *backup* é nativo do próprio sistema operacional do servidor no qual fica o equipamento de *backup* oferece, ele é simples e não oferece muitos recursos para o gerenciamento dos *backups.*

Os *backups* são realizados para o um tipo de mídia específica para *backup* com capacidade de até 80 *Gb*, as mídias são catalogadas apenas com o nome da mesma e não possuem uma identificação prática para fácil identificação de conteúdo nas mesmas.

As mídias de *backup* semanal ficam na mesma sala onde estão localizados os servidores, o que expõe a empresa a graves problemas no caso de um incêndio, por exemplo, pois todas as mídias se perderiam.

Soluções propostas:

- Incluir nos *backups* servidores e equipamentos críticos que atualmente não são submetidos a isto;
- Não deixar mídias da semana na mesma sala onde ficam localizados os servidores;
- Criar um mecanismo para validar diariamente os *backups* e conseqüentemente a integridade das mídias;
- Estudar a possibilidade de implantar um sistema de *backup* mais eficiente, principalmente que tenha sistema de recuperação integral de sistemas.

6.2.13 Controle de acesso físico as áreas restritas

O controle de acesso físico é uma prática nos departamentos em que ficam as informações críticas na empresa. Os dois departamentos, que possuem a maior parte das informações críticas da empresa, possuem um bom controle de acesso.

Soluções propostas:

- Evitar que a sala dos servidores fique destrancada quando não houver alguém responsável por perto. Por exemplo, na hora do almoço a sala deve ser trancada com chave e que cada um dos funcionários habilitados a entrar na sala dos servidores tenham uma cópia da chave, aumentado a segurança das informações sem grandes custos.

6.2.14 Combate e prevenção de incêndios

Combate e prevenção de incêndios na empresa é uma preocupação muito grande e bem divulgada entre todos os colaboradores.

Existe na empresa uma brigada de incêndio, na qual participam colaboradores de praticamente todos os turnos, garantindo assim, que em todos os momentos de funcionamento da empresa, tenha um funcionário da brigada presente.

A brigada de incêndio recebe treinamentos periódicos e realiza simulações para os participantes ficarem aptos para trabalharem em diversas situações.

Hidrantes e extintores estão bem dispostos pela empresa e são constantemente verificados, principalmente validades dos extintores.

Os extintores são divididos conforme os riscos oferecidos em cada área, garantindo assim que o tipo ideal para apagar determinado incêndio esteja próximo do local.

Existe também um sistema de alarme para alertar, caso ocorra algum incidente de incêndio ou outro que necessite de uma atenção especial de todos. Há uma lista com os

números de ramais ou telefones importantes, que fica fixada em diversos locais da empresa facilitando a comunicação em caso de algum incidente.

Soluções propostas:

- A Política de Segurança da Informação deve abordar aspectos de combate e prevenção de incêndios.

6.2.15 Triagem de pessoal

A triagem de pessoal está estabelecida em alguns documentos oficiais da área de recursos humanos.

A triagem existente atualmente na empresa se preocupa muito com o ato da contratação dos novos colaboradores, realizando diversas checagens e submetendo os candidatos ao processo correspondente com a área de atuação.

Uma falha que pode ser apontada neste processo é a falta de uma verificação periódica dos colaboradores efetivos, principalmente aqueles que ocupam cargos que manipulam informações críticas, ou que tenham acesso na parte financeira da empresa.

Outro ponto importante neste processo, que não é prática da empresa atualmente, é o acompanhamento de pessoas que são demitidas ou se desligam da empresa, pois como o contrato de confidencialidade da empresa estipula um prazo de dois anos para tal confidencialidade, estas pessoas podem vir a divulgar informações importantes da empresa antes do término deste período.

Soluções propostas:

- Verificar constantemente a situação financeira dos colaboradores que trabalham em departamentos estratégicos e que tenham acesso a informações financeiras e de resultados da empresa. A verificação pode ser feita por intermédio de

consultas a instituições como o SERASA, ou outras instituições que são acionadas pelas empresas para cadastrarem clientes que estão em débitos com elas;

- Criar mecanismos para acompanhar ex-colaboradores, principalmente se não foram transferidos para uma empresa concorrente.

6.2.16 Segurança e tratamento de mídias

A segurança e o tratamento de mídias não estão descritos em nenhuma política ou documento da empresa. No entanto é praticado de maneira isolada em alguns departamentos, principalmente em dados considerados extremamente críticos.

Soluções propostas:

- Incluir na Política de Segurança da Informação um item que especifique como deve ser realizado o tratamento dos diversos tipos de mídia;
- Estar atento com a classificação das informações, pois somente com uma classificação bem feita é possível realizar o descarte correto dos diferentes tipos de mídias e informações.

6.2.17 Palavra dos diretores

Todos os diretores da empresa foram entrevistados, inclusive o Presidente da empresa. As entrevistas foram bastante proveitosas, pois os mesmos foram entrevistados separadamente e cada um pode mostrar o seu conhecimento sobre segurança da informação e o que pensam para o futuro da empresa.

A partir das respostas pode-se observar que todos eles têm conhecimentos sobre o que é segurança da informação de uma maneira bem global.

Os diretores da empresa estão cientes que atualmente a empresa não possui uma gestão de segurança da informação adequada com o que consideram necessário para a mesma, isso ficou muito claro quando questionados sobre a nota que dariam para a segurança da informação atualmente na empresa e a média obtida foi 4,5.

Outro consenso entre os diretores é que a segurança da informação é um ponto importantíssimo para a empresa, principalmente pelo fato do ramo de atividade da empresa ser alimentício/farmacêutico, pois são áreas que merecem uma grande atenção para questões de segurança da informação.

A segurança da informação foi classificada por eles como um forte diferencial competitivo no mercado atual, e que cada vez mais as empresas vão se fortalecer para garantir principalmente a confidencialidade das informações das empresas que trabalham em parceria para grandes e estratégicos projetos.

Segundo os diretores, a área de segurança da informação é uma área que merece maior atenção para os próximos anos e que pretendem investir na medida do possível para melhorá-la. Além de investimentos, todos deixaram claro que para um projeto de segurança da informação dentro da empresa, eles darão total apoio para que novas medidas de segurança da informação sejam implementadas e afirmaram que realmente segurança da informação é uma preocupação da empresa.

6.2.18 Considerações sobre o Estudo de Caso

A Segurança da Informação atualmente na SAF é uma área bastante limitada, ou seja, tem o básico para que a Empresa consiga manter seus recursos de sistemas de informação em funcionamento e sempre disponível.

Os pontos acima listados foram as principais falhas de segurança da informação encontradas atualmente na empresa. Seguindo a orientação da empresa, o foco das soluções apresentadas em sua grande maioria são ações que não dependem de investimentos em recursos tecnológicos e sim de processos que precisam ser melhorados e implementados na empresa.

As soluções apresentadas para a SAF são as bases que a Empresa necessita para elaborar um plano de ação de segurança da informação. Estas soluções podem ser implementadas na empresa sem que haja grandes investimentos em recursos tecnológicos, mas oferece para a Empresa a possibilidade de criar uma estrutura de segurança da informação, fazendo com que seus funcionários tenham no seu dia a dia a cultura de segurança da informação e comecem a perceber que a segurança da informação é um forte diferencial competitivo para a empresa e não apenas uma área que apenas restringe e controla todas as transações dentro da Empresa.

A seguir será apresentada uma tabela contendo os principais problemas encontrados na empresa, seguido das soluções propostas.

Tabela – Problemas e soluções com relação à segurança da informação na empresa SAF.

Política de Segurança da Informação	
Problemas	Soluções
Existência de uma Política desatualizada.	Revisar a Política atual; Criar um Comitê de Segurança da Informação; Realizar um treinamento após a revisão da política; Ministrar o treinamento por um pessoal que tenha amplo conhecimento do assunto; Formalizar que todos têm ciência do que a Política de Segurança da informação rege.
Titularidade das Informações	
Problemas	Soluções
Desconhecimento dos usuários	Realizar uma ampla divulgação da nova Política.
Segurança das Informações	
Problemas	Soluções
Falta de controle efetivo de pessoas que entram e saem da empresa com câmeras digitais, celulares com câmera e dispositivos de armazenamento;	Realizar um controle efetivo de pessoas e funcionários que entram na empresa com dispositivos como: câmeras, celulares com câmera, filmadoras e afins;
Falta de identificação dos gestores de ativos;	Melhorar a identificação dos gestores dos ativos da empresa;
Ausência de um treinamento sobre a importância do ID's e senhas dos usuários;	Fortalecer no treinamento da nova Política a importância do ID e senha de cada usuário;
Não existe controle sobre envio e recebimento de mensagens pelo correio eletrônico;	Adquirir ou desenvolver um sistema que controle o envio/recebimento de mensagens de correio eletrônico e que divida em grupos: os que podem e os que não podem enviar anexos;
Praticamente todas as estações de trabalho possuem unidades de disquete e USB liberados;	Remover das estações de trabalho as unidades de disquete, CD Rom e bloquear as portas do tipo USB;

Problemas	Soluções
Insuficiência de controle sobre a impressão de ordens de produção;	Criar um mecanismo que controle a impressão de ordens de produção e documentos com informações confidenciais;
Falta de cuidado com a impressão de documentos contendo informações estratégicas e confidenciais, que são deixados próximos às impressoras por muito tempo.	Instruir os usuários para não deixarem documentos importantes impressos próximos às impressoras, ou seja, sempre que imprimirem algo buscar em seguida.
Classificação das Informações	
Problemas	Soluções
Não existe a classificação de informações.	Iniciar um trabalho de classificação das informações.
Sigilo das Informações	
Problemas	Soluções
Não há controle no sigilo das informações;	Com a classificação das informações será possível controlar de uma maneira efetiva as informações sigilosas;
Não existe uma política de mesas e telas vazias;	No treinamento da nova Política abordar sobre a importância de não deixar informações importantes espalhadas pela mesa e bloquear a estação de trabalho quando se ausentar.
Autorização para acesso a recursos tecnológicos	
Problemas	Soluções
A liberação do acesso é feita por uma simples mensagem de correio eletrônico ou do sistema de comunicação interna da empresa, enviada pelas pessoas autorizadas.	Criar um mecanismo um pouco mais formal para a solicitação. Por exemplo, um documento específico para a solicitação de novos usuários ou novos acessos.
Proteção contra vírus e softwares maliciosos	
Problemas	Soluções
A atualização do antivírus não é automatizada;	Implantação de um sistema de antivírus do tipo corporativo, o qual oferece mais recursos e maior controle das estações de trabalho;
A prática de recusa de determinados arquivos não é bem difundida pelos usuários.	Deixar claro na nova Política como é estabelecida a recusa de determinados tipos de arquivos e quais são estes tipos e implantar um sistema de anti *spam*.

Procedimentos para acesso a internet	
Problemas	Soluções
Falta de total ciência dos gestores de que podem a qualquer momento solicitar relatórios dos acessos dos usuários que estão sob sua responsabilidade.	Enviar relatórios periódicos para os gestores; Implementar uma ferramenta que gerencie melhor os acessos dos usuários e que consiga fornecer relatórios de uma maneira prática; Controlar os usuários de ferramentas de mensagem instantânea, e a lista de contatos de todos, para evitar desperdício de tempo.

Procedimentos para Correio Eletrônico	
Problemas	Soluções
Não existe um controle efetivo sobre o envio/recebimento de e-mails, principalmente com anexos.	Adquirir ou desenvolver um sistema que seja capaz de controlar o envio/recebimento de mensagens com anexos e definir os usuários que podem enviar mensagens com anexo.

Gerenciamento, controle da rede, monitoração do uso e acesso aos Sistemas	
Problemas	Soluções
Usuários afastados ou de férias não têm seus ID’s bloqueados neste período.	Acrescentar na política que usuários que se afastem do trabalho por qualquer motivo tenha seu usuário bloqueado neste período.

Senhas e processo de *logon*	
Problemas	Soluções
Senhas genéricas;	Não permitir o uso de usuários genéricos;
Senhas sem o tamanho mínimo;	Configurar os sistemas operacionais e demais softwares utilizados pela empresa para não permitirem a criação/alteração de senhas que não cumpram com o comprimento mínimo estipulado pela política;
Sistemas não configurados para rejeitar senhas anteriores;	Configurar os sistemas operacionais e demais softwares utilizados pela empresa para não permitirem o uso de senhas antigas.
Senhas não expiram depois de determinado período;	Configurar os sistemas para bloquearem automaticamente a senha, caso ela seja digitada errada várias vezes conforme definido na política;

Login não é bloqueado depois de um grande tempo de inatividade.	Configurar os sistemas para bloquearem a estação de trabalho automaticamente caso haja um determinado período de inatividade, conforme estabelecido pela política.
***Backup* e Plano de contingência**	
Problemas	Soluções
Alguns servidores ou equipamentos que possuem informações críticas não possuem *backup*;	Incluir nos *backups* servidores e equipamentos críticos que atualmente não são submetidos a isto.
O sistema para realização de *backup* é nativo do próprio sistema operacional do servidor, ele é simples e não oferece muitos recursos;	Estudar a possibilidade de implantar um sistema de *backup* mais eficiente, principalmente que tenha sistema de recuperação integral de sistemas;
As mídias são catalogadas apenas com o nome e não possuem uma identificação prática para fácil identificação do conteúdo.	Criar um mecanismo para validar diariamente os *backups* e conseqüentemente a integridade das mídias;
As mídias de *backup* semanal ficam na mesma sala onde estão localizados os servidores.	Não deixar mídias da semana na mesma sala onde ficam localizados os servidores.
Controle de acesso físico as áreas restritas	
Problemas	Soluções
O controle é bom, porém todo cuidado é pouco.	Evitar que a sala dos servidores fique destrancada quando não houver alguém responsável por perto.
Combate e prevenção de incêndios	
Problemas	Soluções
Ausência de documentação.	Abordar aspectos de combate e prevenção de incêndios na nova Política de Segurança da Informação.
Triagem de pessoal	
Problemas	Soluções
Falta de uma verificação periódica dos colaboradores efetivos, principalmente os da área financeira;	Verificar constantemente a situação financeira dos colaboradores, por meio do SERASA ou qualquer outra instituição;
Falta de acompanhamento de pessoas que são demitidas ou se desligam da empresa.	Criar mecanismos para acompanharem ex-colaboradores.

Segurança e tratamento de mídias	
Problemas	Soluções
Não existe nada documentado na política e nem em qualquer outro documento da empresa;	Incluir na Política de Segurança da Informação uma especificação de como deve ser realizado o tratamento das mídias;
Prática realizada de maneira isolada em alguns departamentos.	Atentar-se com a classificação das informações para realizar o descarte correto das mídias.

7 CONCLUSÃO

Segurança da Informação é uma área que está em evidência no mercado e as empresas estão cada vez mais buscando garantir a segurança de suas informações. A globalização e a rapidez com que as empresas precisam se comunicar fazem com que o volume de informações geradas seja cada vez maior e mais estratégico, tornando a informação um valioso ativo para a empresa.

As empresas buscam cada vez mais diferenciais competitivos no mercado e podem em muitos casos encontrar esse diferencial justamente na Segurança das Informações. Para a empresa SAF a Segurança da Informação foi apontada por seu Presidente e Diretores como um grande diferencial competitivo, pois, garantir para seus clientes e parceiros que as informações de seus projetos estão seguras, aumenta sua credibilidade no mercado, demonstrando respeito e transparência a toda a sua cadeia de relacionamentos.

A Gestão da Segurança da Informação oferece para a empresa inúmeras vantagens e melhorias, mas estas vantagens são na grande maioria relacionada ao nível de gerenciamento que a empresa tem sobre seus funcionários. A Segurança da Informação não possibilita lucros diretos, no entanto evita que a empresa venha a sofrer prejuízos que podem ser imensuráveis.

Para uma empresa ter sucesso na Gestão da Segurança da Informação é necessário que fique atenta em duas grandes áreas que são: os Recursos Tecnológicos e Humanos. Não basta comprar os melhores produtos de Segurança da Informação disponíveis no mercado, colocando apenas tecnologia de ponta, ou seja, dinheiro apenas não é suficiente, é de extrema importância o comprometimento da alta direção bem como que a Segurança da Informação seja inserida na cultura da empresa, para que os funcionários a vivenciem.

Com os funcionários bem treinados e conscientes de suas responsabilidades com a Segurança da Informação para a empresa, certamente as tecnologias posteriormente implementadas apresentarão melhores resultados.

Diante disso a Segurança da Informação apresenta-se não apenas como modismo entre as empresas e sim como uma área realmente necessária, que pode oferecer um diferencial competitivo e principalmente garantirá que sempre que uma informação seja solicitada esta esteja íntegra, disponível e com sua confidencialidade garantida.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Código de Prática para a Gestão da Segurança da Informação. NBR ISO/IEC 17799: São Paulo, 2001.

BuscaLegis.ccj.ufsc.br. Disponível em: <http://www.buscalegis.ufsc.br/arquivos/direito_autoral_programas_comp.htm>.Acesso em: 16 mai. 2006.

Cert.br Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil Disponível em:<http://www.cert.br/stats/incidentes/2006-apr-jun/top-atacantescc.html> Acesso em: 25/09/2006.

Convergência Digital O melhor conteúdo de TI e Telecom da Internet Brasileira.Disponível em:http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?from%5Finfo%5Findex=11&infoid=3578&query=simple&search%5Fby%5Fauthorname=all&search%5Fby%5Ffield=tax&search%5Fby%5Fheadline=false&search%5Fby%5Fkeywords=any&search%5Fby%5Fpriority=all&search%5Fby%5Fsection=all&search%5Fby%5Fstate=all&search%5Ftext%5Foptions=all&sid=3&text=seguran%E7a+da+informa%E7%E3o+no+brasil> Acesso em 04 set 2006.

DIAS, Claudia. **Segurança e Auditoria da Tecnologia da Informação**. 4. ed. Rio de Janeiro: Axcel Books do Brasil, 2000.

FERREIRA, Aurélio Buarque de Holanda, Minidicionário Aurélio da Língua Portuguesa, 4ª Edição, 2002.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de**.Política de Segurança da Informação - Guia Prático para Elaboração e Implementação.** 1 ed.Rio de Janeiro: Ciência Moderna,2006.

FOCO SECURITY. Disponível em: <http://www.focosecurity.com.br/servicos/analise_risco.asp> Acesso em: 30/09/2006

IDG NOW! Tecnologia em primeiro lugar. Disponível em: <http://idgnow.uol.com.br/seguranca/2006/08/18/idgnoticia.2006-08-18.4274651371/IDGNoticia_view> Acesso em 29 ago 2006.

IDG NOW! Tecnologia em primeiro lugar. Disponível em: http://idgnow.uol.com.br/seguranca/2006/06/26/idgnoticia.2006-06-26.1265987913/IDGNoticia_view> Acesso em 30 ago 2006.

InfoSecurity Task Force. Disponível em :<http://www.istf.com.br/> Acesso em: 10/09/2006.

LAUDON, Kenneth C, LAUDON, Jane Price **Sistemas de Informação com Internet**. 4. ed. Rio de Janeiro: LTC-Livros Técnicos e Científicos S. A, 1999.

Módulo Security. Disponível em: <http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=2&objid=393&pagecounter=0&idiom =0 >. Acesso em: 16 mai. 2006.

Módulo Security. Disponível em: <http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=18&objid=21&idiom=0>. Acesso em: 18 mai. 2006.

Next Generation Center. Disponível em:<http:// www.nextg.com.br>. Acesso em: 09 abr. 2006.

Security Experts. Disponível em: <http://www.securityexperts.com.br/modules.php?name=News&file=article&sid=49>Acesso em 14/09/2006.

Sêmola, Marcos.**Gestão da Segurança da Informação**. 2. ed. Rio de Janeiro: Campus, 2003.

Symantec. Disponível em:<http://www.symantec.com.br> Acesso em: 28 set 2006.

TRUE ACCESS Essencial em Segurança da Informação. Disponível em: <http://www.trueaccess.com.br/downl_artigos/artigo%20-%20investimento%20em%20seguranca%20.pdf.> Acesso em: 22 ago.2006.

TRUE ACCESS Essencial em Segurança da Informação. Disponível em: <http://www.trueaccess.com.br/downl_artigos/artigo%20-%20atividades%20da%20gestao%20corporativa%20de%20seguranca.pdf>
Acesso em: 30 ago.2006.

WIKIPÉDIA, A enciclopédia livre. Disponível em:<http://pt.wikipedia.org/wiki/Spam> Acesso em: 20/08/2006.

Glossário

A

Algoritmo
Seqüência de passos necessários para resolver problemas lógicos ou matemáticos. Certos algoritmos de criptografia são usados para codificar ou decodificar arquivos de dados e mensagens, e para assinar documentos digitalmente. Ver Criptografia e Assinatura digital.

Alias
Não há um padrão comumente aceito pela indústria de segurança para os nomes dos vírus de códigos maliciosos móveis. Cada vírus pode ser conhecido por diferentes nomes ou apelidos.

Ameaça combinada
Ou Blended threat – As ameaças combinadas reúnem características de Vírus, worms, cavalos de Tróia e códigos maliciosos e valem-se da vulnerabilidade dos servidores e da Internet para iniciar, transmitir e disseminar ataques. Devido à utilização de diversos métodos e técnicas, as ameaças combinadas podem espalhar-se rapidamente, provocando danos generalizados. Entre as características das ameaças combinadas encontram-se:
- *A geração de danos:* desencadeiam um ataque de recusa de serviço no endereço IP visando, deformam servidores da Web ou inserem programas cavalo de tróia para uma posterior execução.
- *A propagação através de diversos métodos:* procuram vulnerabilidades com o intuito de comprometer os sistemas, incorporando códigos em arquivos HTML dos servidores, infectando os visitantes de sites comprometidos e enviando e-mails não autorizados (com worms anexados) de servidores comprometidos, por exemplo.
- *Os ataques de vários pontos*: as ameaças combinadas injetam códigos maliciosos nos arquivos.exe aumentam o nível de privilégio da conta de convidado (guest), criam compartilhamentos de rede e legíveis, fazem várias alterações no registro e injetam código de script nos arquivos HTML dos Sistemas.
- *A disseminação sem intervenção humana:* verificam a Internet constantemente, em busca de servidores vulneráveis para atacar.
- *A exploração das vulnerabilidades:* aproveita-se de problemas muito conhecidos, como buffers cheios, vulnerabilidades de validação na entrada do http e senhas conhecidas, para ganhar acesso administrativo não autorizado.

Acionador de atividade
Condição que desencadeia a ativação do vírus ou o faz executar sua rotina destrutiva. A atividade de alguns vírus é acionada em uma determinada data.
A de outros pode ser acionada a partir de execução de certos programas ou da disponibilidade de uma conexão com a internet. Ver *Gatilho*

Applet
Miniatura de aplicação transportada pela Internet, especialmente como uma melhoria em uma página Web. Autores freqüentemente embutem applets em páginas HTML como um tipo de programa adicional. Os applets Java são geralmente os únicos que têm acesso permitido a determinadas áreas do sistema do usuário.Ver *Controles ActiveX.*

Antivírus
Programa especificamente desenvolvido para detectar, anular e eliminar vírus de computador.

Arquivo (vírus de)
Vírus que substitui ou anexa-se a arquivos COM e EXE. Eles podem infectar arquivos com extensões SYS, DRV, BIN, OVL e OVY. Os vírus de arquivo infectam um ou mais arquivos onde quer que o arquivo infectado rode. Ver *Vírus.*

Arquivos COM
Tipo de arquivo executável com tamanho limitado a 64 kbytes.Esses arquivos simples são freqüentemente usados por programas utilitários e pequenas rotinas. Como os arquivos COM são executáveis, os vírus podem infectá-los.

Assinatura digital
Código utilizado para verificar a integridade de um texto ou mensagem. Também pode ser utilizado para verificar se o remetente de uma mensagem é mesmo quem dez ser.

Ataque
Ato de tentar desviar dos controles de segurança de um sistema. Um ataque pode ser ativo, tendo por resultado a liberação dos dados. Nota: o fato de um ataque estar acontecendo não significa necessariamente que ele terá sucesso. O nível de sucesso depende da vulnerabilidade do sistema ou da atividade e da eficácia das contramedidas existentes.

Ataque interno
Ataque originado de dentro da rede protegida.

Atividade
Trata-se do código de programa que executa a atividade do vírus. Nem todos os vírus têm atividades - alguns apenas se espalham ou se duplicam- e nem todas as atividades executam ações destrutivas.

Autenticação
Processo de determinar a identidade de um usuário que esteja tentando alcançar um sistema. Verificação de identidade.

Avaliação da ameaça
Consiste em uma classificação da gravidade do vírus, worm ou cavalo de Tróia. Ela leva em conta o dano causado pela ameaça, a rapidez com que ela se dissemina em outros computadores (sua distribuição) e a extensão das infecções registradas.

B

Back door
Falha de segurança de um sistema deixada propositalmente pelo desenvolvedor. Códigos maliciosos podem abrir back doors em computadores dando aceso remoto ao micro contaminado por hackers.

Bipartite (ou bimodal)
Vírus que infecta o setor de boot e arquivos. Ver *Vírus*

Blindado

Vírus que tenta evitar que seu código seja examinado. O vírus pode usar vários métodos para tomar mais difícil o rastreamento, o desmanche e a engenharia reversa de seu código.

Bomba lógica
Código inserido clandestinamente em uma aplicação ou um sistema operacional que leva a realizar alguma atividade destrutiva ou que comprometa a segurança toda vez que condições especificadas são encontradas. Compare com Back door.

Boot
1 - Setor do disco rígido ou de disquetes onde ficam gravadas as informações essenciais de um programa ou do sistema operacional;
2 - Vírus que infecta a primeira trilha do disco lógico e impede o funcionamento correto do sistema.Ver *Vírus.*

Brincalhão
Programa inofensivo que faz o computador executar várias atividades não destrutivas (por exemplo, apresentar de repente uma nova proteção de tela).ver *Vírus.*

Bug
Falha não intencional que provoca mau funcionamento em um programa de computador ou em uma peca de hardware. O termo, que em português significa inseto, é uma referência à primeira falha real encontrada em um computador: uma mariposa que havia se instalado entre os circuitos do computador Mark II, da Universidade de Harvard,causando mau funcionamento.

Buraco ou brecha
Vulnerabilidade na construção do software ou hardware que permite burlar medidas de segurança.

C

Carga viral
Ação que o vírus executa no computador infectado. Pode ser relativamente inócua (como a exibição de mensagens ou a ejeção do drive de CD) ou bastante destrutiva (como o pagamento de todo o conteúdo do disco rígido).

Cavalo de Tróia
Um programa que não se duplica sem se copia, mas provoca danos e compromete a segurança do computador. Normalmente, ele não envia a si mesmo e pode chegar sob a forma de algum software ou programa brincalhão.Ver *Vírus.*

Certificação
Avaliação detalhada das características técnicas e não técnicas da segurança de um sistema e de outras proteções, com base no processo de credenciamento,que estabelece a extensão na qual_um projeto se encontra em relação a um conjunto específico de exigência da segurança.

Chave de registro
O registro do Windows usa chave para armazenar o ambiente de configuração do computado. Quando um usuário instala um novo programa, ou as configurações são alteradas, os valores

dessas chaves mudam. Se um vírus modificar essas chaves,elas poderão produzir efeitos danosos. A edição do registro do Windows só deve ser feita por usuários avançados.

Cluster (vírus de)
Vírus que modifica a tabela de entrada de diretórios para que o vírus seja carregado antes de qualquer outro programa. O código do vírus só existe em um local, mas executar qualquer programa executará o vírus também. Como modificam o diretório, os vírus de cluster parecem infectar todos os programas de um disco. Ver Vírus.

Código malicioso
Programa introduzido intencionalmente no computador do usuário com o objetivo de roubar informações ou derrubar barreiras de segurança. Ver – Cavalo de Tróia;Controles Active X.

Código móvel
Programa (software) transferido do host para o cliente (ou para outro computador Host) a fim de ser executado. Um exemplo de código móvel malicioso é o worm.

Confidencialidade
Propriedade de certas informações que não podem ser disponibilizadas ou divulgadas sem autorização para pessoas, entidades ou processos. O conceito é garantir que a informação sensível seja limitada a um grupo apropriado de pessoas ou organizações.

Controles ActiveX
Módulos de software que adicionam funcionalidades a aplicações baseadas na arquitetura do modelo de objetos da Microsoft. Na Internet, os controles Active-X transformam uma página Web em páginas de software, que agem como qualquer programa carregado a partir de um servidor. Por esse motivo, os controles Active-X podem dar pleno acesso ao sistema. Na maioria das vezes, esse aceso é legítimo, mas programadores mal-intencionados podem usar a tecnologia para aplicações nada nobres. Ver *Applet.*

Cookie
Arquivo de texto armazenado no computador do internauta e que serve para identificar o usuário que visita de novo um site. Um cookie pode conter informações de registro em um site e preferências do usuário. Quando um servidor recebe uma requisição do navegador que inclui um cookie, o servidor pode usar a informação armazenada no arquivo para personalizar o site para o internauta. Os cookies podem ser usados para coletar informações importantes sobre um usuário que seriam impossíveis de obter sem ele.

Correção
Pedaço de código feito para corrigir falhas em um software ou no sistema operacional. Geralmente, as correções são liberadas pelo desenvolvedor do software defeituoso.Ver *Patch.*

Correntes
Corrente de e-mail ou conhecido no Brasil também como *forward*, trata-se de um e-mail que é enviado para diversos conhecidos ao mesmo tempo e que são eventualmente repassadas adiante e na maioria das vezes se espalham em ritmo exponencial por causa do efeito dominó, atingindo assim muitas vezes milhões de pessoas.

Cracker

Pessoa que quebra a segurança de um sistema sem, necessariamente,conhecer seu funcionamento a fundo. Intrometido e malicioso que tente descobrir informações sensíveis bisbilhotando.Ver *Hacker.*

Criptografado
São os que utilizam a criptografia para se esconder dos verificadores de vírus,ou seja, eles desorganizam seu código de programa para dificultar a detecção. Ver *Vírus.*

Criptografia
Conjunto de técnica que permitem embaralhar as informações (mensagens, dados armazenados) transmitidas entre os computadores, de modo a impedir que o conteúdo dessas informações seja lido no meio do caminho. A criptografia é usada para autenticar a identidade de usuários e transações bancárias e proteger transferências eletrônicas de fundos e o sigilo das comunicações pessoais e comerciais. Ver *Encriptação.*

D

Dano
O componente relativo a danos avalia os estragos que uma determinada ameaça pode provocar.Essa avaliação inclui os eventos acionados, a obstrução de servidores de e-mail, a exclusão ou modificação de arquivos, a liberação informações sigilosas, a degradação do desempenho, os erros no código do vírus, o comprometimento das configurações de segurança e a facilidade com a qual os danos podem ser reparados.

Destrutivo
Os vírus d computador podem ter uma rotina que pode acionar a carga viral. Um vírus será definido como destrutivo se sua carga viral causar algum dano ao sistema, como corromper e deletar arquivos, formatar o HD e executar ataques de negação de serviço.

DoS (Denial of Service)
Ou negação de serviço, em português.Trata-se de um ataque com a finalidade de tirar um site ou um servidor do ar. Consiste no envio de milhares de requisições simultâneas a um endereço, sobrecarregando o sistema e impedindo o acesso de usuários reais.

E

Encriptação
Processo de disfarçar a informação de modo que ela não seja compreendida por uma pessoa não autorizada. Ver Criptografia.

Engenharia social
Termo usado para técnicas que apóiam mais em pessoas do que no software. O objetivo é levar funcionários e colaboradores de uma empresa a revelar, por ingenuidade ou confiança, senhas e outras informações que possam comprometer a segurança de um sistema.

Exploração
Quando um programa ou técnica se aproveita de uma vulnerabilidade do software. As explorações podem ser usadas para violar a segurança ou atacar um host através da rede.

F

Firewall
Filtro colocado no computador que funciona como ima barreira contra intrusos ou uso indevido dos recursos do sistema. Pode ser software, hardware ou uma combinação dos dois.

G

Gatilho
Ação ou data que pode acionar o vírus no computador infectado. Os vírus ativados por data podem afetar o computador nos 365 dias do ano, pois podem infectar a máquina antes da data para sua execução.

H

Hacker
Pessoa que gosta de explorar os detalhes e ampliar as capacidades de sistemas programáveis. Ao contrário da maioria dos usuários, que prefere aprender apenas o mínimo necessário, o hacker:
- programa entusiasticamente ou gosta mais de programar do que apenas teorizar sobre programação;
- programa rapidamente;
- é especialista em algum tipo de programa ou que freqüentemente fez seu trabalho usando a especialidade ou baseado nela;
- gosta do desafio intelectual de superar ou driblar limitações.

Ver *Cracker*

Hoax
Vírus falso ou vírus-boato. Normalmente uma mensagem de e-mail enviada sob a forma de "corrente" que descreve algum vírus devastador de existência bastante improvável. É bem fácil identificá-lo porque mão há arquivos anexados, nem o aval de nenhuma autoridade para as declarações de mensagem, e também pelo tom geral da mensagem.Ver *Vírus.*

I

Infecção
Ação que um vírus coloca em prática quando entra em um sistema de computador ou em um dispositivo de armazenamento.

Intrusão
Invasão ou tentativa de invasão de um sistema protegido.

M

Macro
Programa ou segmento de código escrito na linguagem de macro interna de um aplicativo. Algumas macros se duplicam, enquanto outras infectam documentos. Ver *Vírus.*

Malware
Termo genérico usado para descrever códigos maliciosos como vírus, cavalos de Tróia, conteúdo ativo malicioso etc.

P

Patch
Remendo, em português, é um pedaço de software para ser adicionado temporariamente a um programa com a finalidade de corrigir um defeito. Um patch pode ou não funcionar, e pode ou não ser incorporado definitivamente no programa. Ver *Correção.*

PGP
Sigla para Pretty Good Privacy, programa de criptografia que utiliza conceitos de chave pública e chave privada.

Phreaker
Pessoa que quebra a segurança de redes de telefonia.

Polimorfo
Vírus que cria cópias variadas e funcionais de si mesmo como meio de evitar a detecção por softwares antivírus.o mesmo vírus pode parecer completamente diferente em sistemas diferentes ou em arquivos diferentes.Ver *Vírus.*

Proxy
Um servidor que atua como intermediário entre um cliente e outro servidor.Normalmente é utilizado em empresas para aumentar a performance de acesso a determinados serviços ou permitir que mais de uma máquina se conectes e utilizados como uma forma de tornar anônimas algumas ações na Internet, como, por exemplo, atacar outras redes ou enviar SPAM.

R

Replicação
Processo pelo qual um vírus faz cópias de si mesmo com o objetivo de executar infecções subseqüentes. A replicação é um das características que separa os vírus de outros programas de computador.

Residente de memória
Vírus que permanece na memória depois que é executado e infecta outros arquivos quando certas condições são encontradas.Em contraposição, os vírus não residentes ficam ativos somente quando a aplicação infectada está rodando.

Retrovírus
Vírus que desabilitam ou infectam um software antivírus específico.

S

Scam
Falsas mensagens de e-mail enviadas aos usuários utilizando nomes de empresas e serviços conhecidos.Os scams incentivam o usuário a fazer download de arquivos, os quais posteriormente são detectados como worms, cavalos de Tróia ou outras ameaças.Em alguns casos, essas mensagens simulam formulários ou páginas de web referentes a bancos ou outro serviço que exija cadastramento, com o objetivo de capturar informações confidenciais, como,

por exemplo, dados bancários, número de cartão de crédito, nome e endereço, entre outras.Ver *Hoax.*

Senha
Conjunto de caracteres (letras, números e símbolos) de conhecimento exclusivo do usuário.A senha é usada no processo de verificação de identidade.

Sneaker
Indivíduo contratado para invadir lugares com o objetivo de testar a segurança.

Spam
Propaganda não solicitada enviada por e-mail.originalmente, o termo é usado para definir o ato de derrubar um programa ao fazer um buffer de tamanho fixo transbordar por causa de entrada de dados excessivamente grandes.

Spammer
Pessoa que envia mensagens não solicitadas.

Spoofing
Tentativa de ganhar acesso a um sistema fingindo ser um usuário autorizado.

SSL (Secura Sockets Layer)
Protocolo que possibilita realizar comunicações seguras através de criptografia e autenticação.

T

Trojan
Ver *Cavalo de Tróia.*

V

Variante
Novas linhagens de vírus que "tomam emprestado" o código de outros vírus conhecidos, em graus variados.As variantes em geral são identificadas por uma ou mais letras após o "sobrenome" do vírus, como: VBS.LoveLetter:B, VBS.LoveLetter.C etc.

Vírus
Programa ou código que se duplica, ou seja, infecta outro programa, setor de inicialização, setor de partição ou documento que suporta macros inserindo-se ou anexando-se àquela meio. Quando esses programas são executados, o vírus embutido é executado também, propagando a infecção.isso normalmente acontece sem que o usuário da máquina perceba.Ao contrário do worm, um vírus não pode infectar computadores sem ajuda.Ele se propaga usando vetores, como, por exemplo, programas trocados por usuários. Os vírus podem não fazer nada, a não ser propagar-se e deixar o programa infectado funcionar normalmente.Contudo, depois de se propagar silenciosamente por um período, ele começa a exibir mensagens ou pregar peças.

Ver também:
- Criptografado
- Polimorfo ou mutante
- Macro

- Boot
- Hoax (falso)
- Cavalo de Tróia
- Worm
- Arquivo
- Blindado
- Cluster
- Residente de memória

Vulnerabilidade
Qualquer característica de um sistema que permita que alguém o impeça de operar corretamente ou que permita a usuários não autorizados assumirem o controlo sobre ele.

W

Wep
Do inglês Wired equivalente Privacy, protocolo de segurança para redes sem fio que usa a criptografia para a transmissão de dados.

Worm
Programa que faz cópias d si mesmo, por exemplo: de uma unidade de disco para outra, através de e-mail ou outro mecanismo de transporte.ele pode danificar o computador e comprometer sua segurança, apresentando-se sob a forma de algum software ou programa brincalhão.

APÊNDICE A – Questões direcionadas à administração da empresa

Verificação de existência de política de segurança

01. É de seu conhecimento a existência de política de segurança da informação ou algum documento que trate alguns aspectos de segurança?

02. Esse documento é de seu conhecimento?

03. Como foi divulgado este documento no seu departamento?

Titularidade das informações

04. A empresa tem algum documento que estabeleça que a empresa é quem detém todos os direitos sobre toda e qualquer informação que esteja armazena em seus recursos tecnológicos?

05. A empresa possui um documento que estabelece que ela possa a qualquer momento acessar qualquer informação armazenada nos seus recursos tecnológicos É de seu conhecimento este documento

Segurança das informações

06. A política da empresa define que cada funcionário é responsável direto ou indireto pela segurança das informações na empresa È de seu conhecimento este procedimento?

07. Você já recebeu algum treinamento falando sobre a importância da confidencialidade de seu usuário e senha nos sistemas?

08. Existe na empresa um documento que prevê que os usuários podem vir a serem punidos caso seja identificado que de alguma maneira tenta burlar ou desabilitar os recursos de segurança da empresa É de seu conhecimento este documento?

09. Atualmente são identificados os gestores de todos os ativos relevantes, e atribuídas as responsabilidades pela manutenção de controles apropriados?

10. É feito inventário de ativos na empresa?

11. A empresa oferece níveis de proteção compatíveis com o valor e a importância dos ativos?

12. A organização é capaz de identificar os seus ativos e saber o valor relativo e a importância dos mesmos?

13. É elaborado e mantido um inventário dos ativos importantes associados a cada sistema de informação?

14. É evitado o trabalho não supervisionado em áreas seguras, tanto por motivo de segurança como para não dar oportunidade a atividades mal intencionadas?

15. É proibida a presença de equipamento fotográfico, de vídeo, áudio ou gravação, a não ser com autorização?

16. A organização estabelece uma política referente aos atos de comer, beber e fumar nas instalações de processamento de informações, locais restritos ou próximos a materiais inflamáveis?

Classificação das informações

17. Existe uma classificação das informações para assegurar que os ativos de informação recebam um nível de proteção adequado?

18. Sabendo-se que algumas informações são mais sensíveis e criticas do que outras e que alguns itens podem exigir um nível adicional de proteção ou manuseio especial tem sido utilizado um sistema de classificação para definir um conjunto apropriado de níveis de proteção e comunicar a necessidade de medidas especiais de manuseio?

19. As informações são rotuladas para indicar até que ponto são criticas para a empresa, quanto à sua integridade e disponibilidade?

Sigilo das informações

20. A empresa estabelece regras para a saída de informações confidenciais da empresa?

21. Existe controle sobre o envio de informações confidenciais?

22. É permitido o envio deste tipo de informação pelo correio eletrônico? Isto é controlado?

23. São definidos os colaboradores que devem ter acesso às informações confidenciais dentro do departamento?

24. Existe política de mesa vazia e tela vazia para reduzir o risco de acessos não autorizados ou danos a documentos, mídia e instalações de processamento de informações?

Autorização para uso de recursos tecnológicos

25. Os acessos aos recursos tecnológicos são definidos conforme a necessidade de cada usuário?

26. A política define a hierarquia para solicitações de acessos? Esta hierarquia é utilizada na prática dentro do seu departamento?

27. A política estabelece que quando os usuários deixarem suas estações de trabalho eles devem bloquear as mesmas para evitar acessos não autorizados? Isso é praticado? Se não qual o motivo?

28. Nas estações de trabalho são instalados apenas os aplicativos referentes à tarefa do seu departamento?

29. Você tem permissão para fazer downloads e instalação de softwares em sua estação de trabalho?

30. É de seu conhecimento a hierarquia para solicitação de usuário ou novos acessos?

Proteção contra software malicioso e vírus

31. Seu computador possui um software de antivírus instalado?

32. A atualização do antivírus é automática? Depende de alguma ação sua para atualizar?

33. Você recebeu algum tipo de treinamento para a utilização correta do antivírus?

34. A política da empresa estabelece o direito de recusa de determinados tipos de anexos ou conteúdos contidos nas mensagens de correio eletrônico É de seu conhecimento que determinados arquivos não são permitidos enviar e receber?

35. A política estabelece que todos os softwares da empresa são homologados e todos os direitos sobre os mesmos são da empresa e que nenhum funcionário pode realizar upload (enviar) de softwares

Procedimentos para acesso à internet

36. Existe uma política de acesso à internet? É de seu conhecimento?

37. Para a utilização da internet é necessário um ID e uma senha? Alguém tem conhecimento de seu ID e senha?

38. Existe controle de conteúdo permitido acessar na Internet? É de seu conhecimento como isto é estabelecido?

39. Existe monitoramento sobre os acessos dos usuários É de seu conhecimento este monitoramento?

40. Você já recebeu algum treinamento sobre como utilizar a internet de maneira segura e produtiva?

Procedimentos para uso de correio eletrônico

41. Existe uma política para a utilização de correio eletrônico É de conhecimento de seu conhecimento?

42. Quem é o proprietário dos e-mails que você envia e recebe?

43. A política estabelece que não é permitido o uso do correio eletrônico corporativo para fins particulares É de seu conhecimento?

44. Existe algum treinamento sobre como utilizar o correio eletrônico de maneira adequada à política da empresa?

Gerenciamento, controle da rede, monitoração do uso e acesso aos sistemas

45. Todas as solicitações de acesso são formais e liberadas conforme a hierarquia definida na política? Isso é controlado no departamento?

46. Existe revisão periódica dos acessos?

Identificação e autenticação do usuário, senhas e processo de logon

47. A identificação do usuário é individual? Existem senhas genéricas no departamento?

48. Existe um número mínimo de caracteres para a criação de senha?

Controle de acesso físico e proteção física as áreas restritas

49. Existe controle de acesso à sala em que estão os documentos de desenvolvimento?

50. Existe monitoramento por circuito fechado de TV às áreas em que são armazenadas as informações confidenciais do departamento?

51. Existe sistema de combate a incêndio próximo a sala em que estão armazenadas as informações confidenciais?

52. Existe sistema de detecção de fumaça?

Segurança e tratamento de mídias

53. Existem procedimentos para descarte de mídias (CDs, impressos, disquetes, Hds, etc)? É de conhecimento de todos do departamento?

APÊNDICE B – Questões direcionadas à diretoria da empresa

01. O que o Sr. (a) entende por segurança da informação? (questionar sobre abrangência e processos)

02. Em reuniões, eventos, visitas e bate papos em geral com outros empresários já conversaram sobre segurança da informação?

03. Qual a importância da segurança da informação no ramo de atividade da empresa?

04. O Sr (a). têm conhecimento de algum documento que trate aspectos de segurança da informação na empresa?

05. Em uma escala de 0 a 10 qual nota daria para a segurança da informação da empresa?

06. No segmento da empresa, tem noção se o que existe de segurança em sua empresa é compatível com o da concorrência?

07. Na sua visão de quem é a responsabilidade pela segurança da informação?

08. Considera que a segurança da informação pode ser um diferencial competitivo da empresa? Justifique.

09. Acha que a empresa já sofreu algum tipo de “ataque”?

10. Atualmente, a informação é um ativo de grande valor para as empresas e cada vez mais deve ser protegida como ou até melhor que qualquer outro ativo da empresa. Qual sua perspectiva para a segurança da informação dentro de sua empresa nos próximos cinco anos?

APÊNDICE C – Questões direcionadas ao departamento industrial da empresa

Verificação de existência de política de segurança

01. É de seu conhecimento a existência de política de segurança da informação ou algum documento que trate alguns aspectos de segurança?

02. Esse documento é de seu conhecimento?

03. Como foi divulgado este documento no seu departamento?

Titularidade das informações

04. A empresa tem algum documento que estabeleça que a empresa é quem detém todos os direitos sobre toda e qualquer informação que esteja armazenada em seus recursos tecnológicos?

05. A empresa possui um documento que estabelece que ela pode a qualquer momento acessar qualquer informação armazenada nos seus recursos tecnológicos. É de seu conhecimento este documento?

Segurança das informações

06. A política da empresa define que cada funcionário é responsável direto ou indireto pela segurança das informações na empresa. É de seu conhecimento este procedimento?

07. Você já recebeu algum treinamento falando sobre a importância da confidencialidade de seu usuário e senha nos sistemas?

08. Existe na empresa um documento que presume que qualquer usuário possa vir a ser punido caso seja identificado que de alguma maneira tenta burlar ou desabilitar os recursos de segurança da empresa? É de seu conhecimento este documento?

09. Atualmente são identificados os gestores de todos os ativos relevantes e são atribuídas as responsabilidades pela manutenção de controles apropriados?

10. É evitado o trabalho não supervisionado em áreas seguras, tanto por motivo de segurança como para não dar oportunidade a atividades mal intencionadas?

11. As áreas seguras desocupadas são trancadas fisicamente e inspecionadas periodicamente?

12. É proibida a presença de equipamento fotográfico, de vídeo, áudio ou gravação, a não ser com autorização?

13. O material recebido é inspecionado para detectar eventuais perigos antes de ser transportado da área de armazenagem provisória para o local de utilização?

14. A organização estabelece uma política referente aos atos de comer, beber e fumar nas instalações de processamento de informações, locais restritos ou próximos a materiais inflamáveis?

15. Existe controle sobre a impressão de ordens de produção?

16. Se a ordem for perdida e o operador solicitar uma nova ordem, existe controle sobre este procedimento?

17. No caso de uma nova solicitação de ordem é exigido que traga a ordem velha, mesmo que seja rasgada, suja ou com danos ao documento?

18. Na ordem de produção vem escrita a fórmula de como fazer o produto ?

Classificação das informações

19. Existe uma classificação das informações para assegurar que os ativos de informação recebam um nível de proteção adequado?

20. Sabendo-se que algumas informações são mais sensíveis e críticas do que outras e que alguns itens podem exigir um nível adicional de proteção ou manuseio especial, tem sido utilizado um sistema de classificação para definir um conjunto apropriado de níveis de proteção e comunicar a necessidade de medidas especiais de manuseio?

21. As informações são rotuladas para indicar até que ponto elas são criticas para a empresa, quanto à sua integridade e disponibilidade?

Sigilo das informações

22. A empresa estabelece regras para a saída de informações confidenciais da empresa?

23. Existe controle sobre o envio de informações confidenciais?

24. É permitido o envio deste tipo de informação pelo correio eletrônico? Isto é controlado?

25. São definidos os colaboradores que devem ter acesso às informações confidenciais dentro do departamento?

26. Existe política de mesa vazia e tela vazia para reduzir o risco de acessos não autorizados ou danos a documentos, mídia e instalações de processamento de informações?

Autorização para uso de recursos tecnológicos

27. Os acessos aos recursos tecnológicos são definidos conforme a necessidade de cada usuário?

28. A política define a hierarquia para solicitações de acessos? Esta hierarquia é utilizada na prática dentro do seu departamento?

29. A política estabelece que quando os usuários deixarem suas estações de trabalho eles devem bloquear as mesmas para evitar acessos não autorizados? Isso é praticado? Caso não seja qual o motivo?

30. Nas estações de trabalho são instalados apenas os aplicativos referentes à tarefa do seu departamento?

31. Você tem permissão para fazer downloads e instalação de softwares em sua estação de trabalho?

32. É de seu conhecimento a hierarquia para solicitação de usuário ou novos acessos?

Proteção contra software malicioso e vírus

33. Seu computador possui um software de anti-vírus instalado?

34. A atualização do antivírus é automática ou depende de alguma ação sua para atualizar?

35. Você recebeu algum tipo de treinamento para a utilização correta do anti-vírus?

36. A política da empresa estabelece o direito de recusa de determinados tipos de anexos ou conteúdos contidos nas mensagens de correio eletrônico. É de seu conhecimento que determinados arquivos não são permitidos enviar e receber?

37. A política estabelece que todos os softwares da empresa são homologados e todos os direitos sobre os mesmos são da empresa e que nenhum funcionário pode realizar upload (enviar) de softwares?

Procedimentos para acesso à internet

38. Existe uma política de acesso à internet? É de seu conhecimento?

39. Para a utilização da internet é necessário um ID e uma senha. Alguém tem conhecimento de seu ID e senha?

40. Existe controle de conteúdo que é permitido acessar na internet. É de seu conhecimento? Como isso é estabelecido?

41. Existe monitoramento sobre os acessos dos usuários. É de seu conhecimento este monitoramento?

42. Você já recebeu algum treinamento sobre como utilizar a internet de maneira segura e produtiva?

Procedimentos para uso de correio eletrônico

43. Existe uma política para a utilização de correio eletrônico. É de seu conhecimento?

44. Quem é o proprietário dos e-mails que você envia e recebe?

45. A política estabelece que não é permitido o uso do correio eletrônico corporativo para fins particulares. É de seu conhecimento?

46. Existe algum treinamento sobre como utilizar o correio eletrônico de maneira adequada à política da empresa?

Gerenciamento, controle da rede, monitoração do uso e acesso aos sistemas.

47. Todas as solicitações de acesso são formais e liberadas conforme a hierarquia definida na política? Isso é controlado no departamento?

48. Existe revisão periódica dos acessos?

Identificação e autenticação do usuário, senhas e processo de logon

49 . A identificação do usuário é individual? Existem senhas genéricas no departamento?

50 . Existe um número mínimo de caracteres para a criação de senha?

Controle de acesso físico e proteção física as áreas restritas

51 . Existe controle de acesso à sala em que estão os documentos de desenvolvimento?

52 . Existe monitoramento por circuito fechado de TV às áreas em que são armazenadas as informações confidenciais do departamento?

53 . Existe sistema de combate a incêndio próximo a sala em que estão armazenadas as informações confidenciais?

54 . Existe sistema de detecção de fumaça?

55 . Materiais perigosos ou combustíveis são armazenados de modo seguro e a uma distância adequada?

56 . Os suprimentos em grande volume são armazenados dentro de uma área segura, somente sendo requisitados à medida que forem sendo utilizados?

Segurança e tratamento de mídias

57. Existem procedimentos para descarte de mídias (CDs, impressos, disquetes, Hds, etc)? É de conhecimento de todos do departamento?

APÊNDICE D – Questões direcionadas ao departamento de pesquisa e desenvolvimento da empresa

Verificação de existência de política de segurança

01. É de seu conhecimento a existência de política de segurança da informação ou algum documento que trate alguns aspectos de segurança?

02. Esse documento é de seu conhecimento?

03. Como foi divulgado este documento no seu departamento?

Titularidade das informações

04. A empresa tem algum documento que estabeleça que a empresa é quem detêm todos os direitos sobre toda e qualquer informação que esteja armazenada em seus recursos tecnológicos?

05. A empresa possui um documento que estabelece que ela possa a qualquer momento acessar qualquer informação armazenada nos seus recursos tecnológicos. É de seu conhecimento este documento?

Segurança das informações

06. A política da empresa define que cada funcionário é responsável direto ou indireto pela segurança das informações na empresa. É de seu conhecimento este procedimento?

07. Você já recebeu algum treinamento falando sobre a importância da confidencialidade de seu usuário e senha nos sistemas?

08. Existe na empresa um documento que prevê que qualquer usuário pode vir a ser punido caso seja identificado que de alguma maneira tentou burlar ou desabilitar os recursos de segurança da empresa? É de seu conhecimento este documento?

09. Atualmente são identificados os gestores de todos os ativos relevantes, e atribuída a responsabilidade pela manutenção de controles apropriados?

10. É evitado o trabalho não supervisionado em áreas seguras, tanto por motivo de segurança como para não dar oportunidade a atividades mal intencionadas?

11. As áreas seguras desocupadas são trancadas fisicamente e inspecionadas periodicamente?

12. É proibida a presença de equipamento fotográfico, de vídeo, áudio ou gravação, a não ser com autorização?

13. A organização estabelece uma política referente aos atos de comer, beber e fumar nas instalações de processamento de informações, locais restritos ou próximos a materiais inflamáveis?

Classificação das informações

14. Existe uma classificação das informações para assegurar que os ativos de informação recebam um nível de proteção adequado?

15. Sabendo-se que algumas informações são mais sensíveis e críticas do que outras e que alguns itens podem exigir um nível adicional de proteção ou manuseio especial, tem sido utilizado um sistema de classificação para definir um conjunto apropriado de níveis de proteção e comunicar a necessidade de medidas especiais de manuseio?

16. As informações e as saídas produzidas por sistemas que processam dados, são rotuladas quanto ao seu valor e grau de sensibilidade para a empresa?

17. As informações são rotuladas para indicar até que ponto elas são criticas para a empresa, quanto à sua integridade e disponibilidade?

18. As diretrizes de classificação levam em conta e prevêem o fato de que a classificação de um determinado item de informação não é necessariamente imutável no tempo e que pode mudar de acordo com uma política pré-determinada?

19. A responsabilidade pela definição da classificação de uma determinada informação e pela revisão periódica desta classificação é delegada da pessoa que originou a informação ou do gestor designado da informação?

20. São abrangidos os ativos de informação tanto em formato físico quanto em formato eletrônico?

21. Para cada classificação são definidos procedimentos de manuseio referentes a tipos de atividade de processamento da informação como: cópia, armazenagem, transmissão (oral, e-mail, telefone, correio, celular) e descarte de mídias?

22. Os itens a serem levados em conta incluem relatórios impressos, display na tela, informações gravadas (fita, disco, CD Rom), mensagens eletrônicas e transferência de arquivos?

23. Etiquetas físicas (geralmente meio mais apropriado) são utilizadas na rotulagem?

Sigilo das informações

24. A empresa estabelece regras para a saída de informações confidenciais da empresa?

25. Existe controle sobre o envio de informações confidenciais?

26. É permitido o envio deste tipo de informação pelo correio eletrônico? Isto é controlado?

27. São definidos os colaboradores que devem ter acesso às informações confidenciais dentro do departamento?

28. Existe política de mesa vazia e tela vazia para reduzir o risco de acessos não autorizados ou danos à documentos, mídia e instalações de processamento de informações?

Autorização para uso de recursos tecnológicos

29. Os acessos aos recursos tecnológicos são definidos conforme a necessidade de cada usuário?

30. A política define a hierarquia para solicitações de acessos? Esta hierarquia é utilizada na prática dentro do seu departamento?

31. A política estabelece que quando os usuários deixarem suas estações de trabalho eles devem bloquear as mesmas para evitar acessos não autorizados? Isso é praticado? Caso não seja qual o motivo?

32. Nas estações de trabalho são instalados apenas os aplicativos referentes à tarefa do seu departamento?

33. Você tem permissão para fazer downloads e instalação de softwares em sua estação de trabalho?

34. É de seu conhecimento a hierarquia para solicitação de usuário ou novos acessos?

Proteção contra software malicioso e vírus

35. Seu computador possui um software de anti-vírus instalado?

36. A atualização do anti-vírus é automática ou depende de alguma ação sua para atualizar?

37. Você recebeu algum tipo de treinamento para a utilização correta do anti-vírus?

38. A política da empresa estabelece o direito de recusa de determinados tipos de anexos ou conteúdos contidos nas mensagens de correio eletrônico? É de seu conhecimento que determinados arquivos não são permitidos enviar e receber?

39. A política estabelece que todos os softwares da empresa são homologados e todos os direitos sobre os mesmos são da empresa e que nenhum funcionário pode realizar upload (enviar) de softwares.

Procedimentos para acesso à internet

40. Existe uma política de acesso à internet? É de seu conhecimento?

41. Para a utilização da internet é necessário um ID e uma senha? Alguém tem conhecimento de seu ID e senha?

42. Existe controle de conteúdo que é permitido acessar na Internet? É de seu conhecimento como isto é estabelecido?

43. Existe monitoramento sobre os acessos dos usuários? É de seu conhecimento este monitoramento?

44. Você já recebeu algum treinamento sobre como utilizar a internet de maneira segura e produtiva?

Procedimentos para uso de correio eletrônico

45. Existe uma política para a utilização de correio eletrônico. É de seu conhecimento?

46. Quem é o proprietário dos e-mails que você envia e recebe?

47. A política estabelece que não é permitido o uso do correio eletrônico corporativo para fins particulares? É de seu conhecimento?

48. Existe algum treinamento sobre como utilizar o correio eletrônico de maneira adequada à política da empresa?

Gerenciamento, controle da rede, monitoração do uso e acesso aos sistemas.

49. Todas as solicitações de acesso são formais e liberadas conforme a hierarquia definida na política? Isso é controlado no departamento?

50. Existe revisão periódica dos acessos?

Identificação e autenticação do usuário, senhas e processo de logon

51. A identificação do usuário é individual? Existem senhas genéricas no departamento?

52. Existe um número mínimo de caracteres para a criação de senha?

Controle de acesso físico e proteção física as áreas restritas

53. Existe controle de acesso à sala em que estão os documentos de desenvolvimento?

54. Existe monitoramento por circuito fechado de TV às áreas em que são armazenadas as informações confidenciais do departamento?

55. Existe sistema de combate a incêndio próximo a sala em que estão armazenadas as informações confidenciais?

56. Existe sistema de detecção de fumaça?

57. O grau de proteção é proporcional aos riscos identificados?

Segurança e tratamento de mídias

58. Existem procedimentos para descarte de mídias (CDs, impressos, disquetes, Hds, etc)? É de conhecimento de todos do departamento?

APÊNDICE E – Questões direcionadas ao departamento de qualidade da empresa

Verificação de existência de política de segurança

01. É de seu conhecimento a existência de política de segurança da informação ou algum documento que trate alguns aspectos de segurança?

02. Esse documento é de seu conhecimento?

03. Como foi divulgado este documento no seu departamento?

Titularidade das informações

04. A empresa tem algum documento que estabeleça que a empresa é quem detêm todos os direitos sobre toda e qualquer informação que esteja armazenada em seus recursos tecnológicos?

05. A empresa possui um documento que estabelece que a mesma pode a qualquer momento acessar qualquer informação armazenada nos seus recursos tecnológicos. É de seu conhecimento este documento?

Segurança das informações

06. A política da empresa define que cada funcionário é responsável direto ou indireto pela segurança das informações na empresa. É de seu conhecimento este procedimento?

07. Você já recebeu algum treinamento falando sobre a importância da confidencialidade de seu usuário e senha nos sistemas?

08. Existe na empresa um documento que prevê que qualquer usuário possa vir a ser punido caso seja identificado que de alguma maneira tentou burlar ou desabilitar os recursos de segurança da empresa. É de seu conhecimento este documento?

09. Atualmente são identificados os gestores de todos os ativos relevantes, e atribuída a responsabilidade pela manutenção de controles apropriados?

10. Existe uma classificação das informações para assegurar que os ativos de informação recebem um nível de proteção adequado?

Sigilo das informações

11. A empresa estabelece regras para a saída de informações confidenciais da empresa?

12. Existe controle sobre o envio de informações confidenciais?

13. É permitido o envio deste tipo de informação pelo correio eletrônico? Isto é controlado?

14. São definidos os colaboradores que devem ter acesso às informações confidenciais dentro do departamento?

15. É evitado o trabalho não supervisionado em áreas seguras, tanto por motivo de segurança quanto para não dar oportunidade a atividades mal intencionadas?

16. As áreas seguras desocupadas são trancadas fisicamente e inspecionadas periodicamente?

17. É proibida a presença de equipamento fotográfico, de vídeo, áudio ou gravação, a não ser com autorização?

18. A organização estabelece uma política referente aos atos de comer, beber e fumar nas instalações de processamento de informações, locais restritos ou próximos a materiais inflamáveis?

Classificação das informações

19. Existe uma classificação das informações para assegurar que os ativos de informação recebam um nível de proteção adequado?

20. Sabendo-se que algumas informações são mais sensíveis e críticas do que outras e que alguns itens podem exigir um nível adicional de proteção ou manuseio especial, tem sido utilizado um sistema de classificação para definir um conjunto apropriado de níveis de proteção, e comunicar a necessidade de medidas especiais de manuseio?

21. As informações e as saídas produzidas por sistemas que processam dados, são rotuladas quanto ao seu valor e grau de sensibilidade para a empresa?

22. As informações são rotuladas para indicar até que ponto elas são críticas para a empresa, quanto à sua integridade e disponibilidade?

23. As diretrizes de classificação levam em conta e prevêem o fato de que a classificação de um determinado item de informação não é necessariamente imutável no tempo, e que pode mudar de acordo com uma política pré-determinada?

24. A responsabilidade pela definição da classificação de uma determinada informação e pela revisão periódica desta classificação é delegada da pessoa que originou a informação ou do gestor designado da informação?

25. São abrangidos os ativos de informação tanto em formato físico quanto em formato eletrônico?

26. Para cada classificação são definidos procedimentos de manuseio referentes a tipos de atividade de processamento da informação como: cópia, armazenagem, transmissão (oral, e-mail, telefone, correio, celular) e descarte de mídias?

27. Os itens a serem levados em conta incluem: relatórios impressos, display na tela, informações gravadas (fita, disco, CD ROM), mensagens eletrônicas e transferência de arquivos?

28. Etiquetas físicas (geralmente meio mais apropriado) são utilizadas na rotulagem?

Autorização para uso de recursos tecnológicos

29. Os acessos aos recursos tecnológicos são definidos conforme a necessidade de cada usuário?

30. A política define a hierarquia para solicitações de acessos? Esta hierarquia é utilizada na prática dentro do seu departamento?

31. A política estabelece que quando os usuários deixarem suas estações de trabalho eles devem bloquear as mesmas para evitar acessos não autorizados? Isso é praticado? Caso não seja, qual o motivo?

32. Nas estações de trabalho são instalados apenas os aplicativos referentes à tarefa do seu departamento?

33. Você tem permissão para fazer downloads e instalação de softwares em sua estação de trabalho?

34. É de seu conhecimento a hierarquia para solicitação de usuário ou novos acessos?

35. Existe política de mesa vazia e tela vazia para reduzir o risco de acessos não autorizados ou danos à documentos, mídia e instalações de processamento de informações?

Proteção contra software malicioso e vírus

36. Seu computador possui um software de anti-vírus instalado?

37. A atualização do anti-vírus é automática ou depende de alguma ação sua para atualizar?

38.Você recebeu algum tipo de treinamento para a utilização correta do anti-vírus?

39. A política da empresa estabelece o direito de recusa de determinados tipos de anexos ou conteúdos contidos nas mensagens de correio eletrônico? É de seu conhecimento que determinados arquivos não são permitidos enviar e receber?

40. A política estabelece que todos os softwares da empresa são homologados e todos os direitos sobre os mesmos são da empresa e que nenhum funcionário pode realizar upload (enviar) de softwares.

Procedimentos para acesso à internet

41. Existe uma política de acesso à internet? É de seu conhecimento?

42. Para a utilização da internet é necessário um ID e uma senha/ Alguém tem conhecimento de seu ID e senha?

43. Existe controle do conteúdo que é permitido acessar na Internet? É de seu conhecimento? Como isto é estabelecido?

44. Existe monitoramento sobre os acessos dos usuários. É de seu conhecimento este monitoramento?

45. Você já recebeu algum treinamento sobre como utilizar a internet de maneira segura e produtiva?

Procedimentos para uso de correio eletrônico

46. Existe uma política para a utilização de correio eletrônico. É de seu conhecimento?

47. Quem é o proprietário dos e-mails que você envia e recebe?

48. A política estabelece que não é permitido o uso do correio eletrônico corporativo para fins particulares. É de seu conhecimento?

49. Existe algum treinamento sobre como utilizar o correio eletrônico de maneira adequada à política da empresa?

Gerenciamento, controle da rede, monitoração do uso e acesso aos sistemas.

50. Todas as solicitações de acesso são formais e liberadas conforme a hierarquia definida na política? Isso é controlado no departamento?

51. Existe revisão periódica dos acessos?

Identificação e autenticação do usuário, senhas e processo de logon

52. A identificação do usuário é individual? Existem senhas genéricas no departamento?

53. Existe um número mínimo de caracteres para a criação de senha?

Controle de acesso físico e proteção física as áreas restritas

54. Existe controle de acesso à sala em que estão os documentos de desenvolvimento?

55. Existe monitoramento por circuito fechado de TV às áreas em que são armazenadas as informações confidenciais do departamento?

56. Existe sistema de combate a incêndio próximo à sala em que estão armazenadas as informações confidenciais?

57. Existe sistema de detecção de fumaça?

Segurança e tratamento de mídias

58. Existem procedimentos para descarte de mídias (CDs, impressos, disquetes, Hds, etc)? É de conhecimento de todos do departamento?

APÊNDICE F – Questões direcionadas ao departamento de tecnologia da informação da empresa

Verificação de existência de política de segurança

01 . Existe alguma política de segurança da informação ou algum documento que trate alguns aspectos de segurança?

02. Esse documento é de conhecimento de todos na empresa? Desde a alta direção até os cargos menores?

03. Como foi realizada a divulgação deste documento?

Titularidade das informações

04. A empresa tem alguma política ou documento que estabeleça que a empresa é quem detêm todos os direitos sobre toda e qualquer informação que esteja armazenada em seus recursos tecnológicos?

05. A política da empresa estabelece que a mesma pode a qualquer momento acessar qualquer informação armazenada nos seus recursos tecnológicos?

06. Estes documentos são de conhecimento de todos?

Segurança das informações

07. A política da empresa define que cada funcionário é responsável direto e indireto pela segurança das informações na empresa?

08. Os usuários são orientados quanto à importância da privacidade de seus logins e senhas?

09. Colaboradores que de alguma maneira tentar burlar ou desabilitar algum recurso de segurança pode ser penalizado? Está definido na política?

10. É mantida uma proteção apropriada dos ativos da organização?

11. Atualmente são identificados os gestores de todos os ativos relevantes, e atribuída à responsabilidade pela manutenção de controles apropriados?

12. É feito inventário de ativos na empresa?

13. A empresa oferece níveis de proteção compatíveis com o valor e a importância dos ativos?

14. A organização é capaz de identificar os seus ativos e saber o valor relativo e a importância dos mesmos?

15. É elaborado e mantido um inventário dos ativos importantes associados a cada sistema de informação?

16. É evitado o trabalho não supervisionado em áreas seguras, tanto por motivo de segurança quanto para não dar oportunidade à atividades mal intencionadas?

17. As áreas seguras desocupadas são trancadas fisicamente e inspecionadas periodicamente?

18. É proibida a presença de equipamento fotográfico, de vídeo, áudio ou gravação, a não ser com autorização?

19. A organização estabelece uma política referente aos atos de comer, beber e fumar nas instalações de processamento de informações, locais restritos ou próximos a materiais inflamáveis?

20. São monitoradas as condições ambientais quanto a fatores que poderiam afetar negativamente a operação dos equipamentos de processamento de informações?

Classificação das informações

21. Existe uma classificação das informações para assegurar que os ativos de informação recebam um nível de proteção adequado?

22. A classificação da informação indica a necessidade, as prioridades e o grau de proteção?

23. Sabendo-se que algumas informações são mais sensíveis e críticas do que outras e que alguns itens podem exigir um nível adicional de proteção ou manuseio especial, tem sido utilizado um sistema de classificação para definir um conjunto apropriado de níveis de proteção, e comunicar a necessidade de medidas especiais de manuseio?

24. As informações e as saídas produzidas por sistemas que processam dados, são rotuladas quanto ao seu valor e grau de sensibilidade para a empresa?

25. As informações são rotuladas para indicar até que ponto elas são criticas para a empresa, quanto à sua integridade e disponibilidade?

26. As diretrizes de classificação levam em conta e prevêem o fato de que a classificação de um determinado item de informação não é necessariamente imutável no tempo e que pode mudar de acordo com uma política pré-determinada?

27. A responsabilidade pela definição da classificação de uma determinada informação e pela revisão periódica desta classificação é delegada da pessoa que originou a informação ou do gestor designado da informação?

28. São abrangidos os ativos de informação tanto em formato físico quanto em formato eletrônico?

29. Para cada classificação são definidos procedimentos de manuseio referentes a tipos de atividade de processamento da informação como: cópia, armazenagem, transmissão (oral, e-mail, telefone, correio, celular) e descarte de mídias?

30. Os itens a serem levados em conta incluem relatórios impressos, display na tela, informações gravadas (fita, disco, CD ROM), mensagens eletrônicas e transferência de arquivos?

31. Etiquetas físicas (geralmente meio mais apropriado) são utilizadas na rotulagem?

Sigilo das informações

32. A política estabelece regras para a saída de informações confidenciais da empresa?

33. Existe controle sobre o envio de informações confidenciais?

34. É permitido o envio deste tipo de informação pelo correio eletrônico? Isto é controlado?

35. São definidos os colaboradores que devem ter acesso às informações confidenciais?

36. Existe algum termo de confidencialidade quando funcionários são contratados?

Autorização para uso de recursos tecnológicos

37. Os acessos aos recursos tecnológicos são definidos conforme a necessidade de cada usuário?

38. A política define a hierarquia para solicitações de acessos? Esta hierarquia é utilizada na prática?

39. A política estabelece que quando os usuários deixarem suas estações de trabalho eles devem bloquear as mesmas para evitar acessos não autorizados? Isso é praticado?

40. Nas estações de trabalho são instalados apenas os aplicativos referentes à tarefa de cada departamento?

41. Existe controle sobre a instalação de novos softwares nas estações de trabalhos? Como é este controle?

42. Os usuários têm a permissão para fazer downloads e instalação de softwares?

43. É de conhecimento de todos a definição da hierarquia de liberação de acesso?

44. Os dispositivos de entrada e saída das estações de trabalho (USB, disquete, CD) são bloqueados? Existe controle sobre o que entra e sai na empresa através destes dispositivos?

45. Estações de trabalho móveis como notebooks e laptops têm um tratamento especial com relação à segurança das informações? Como isso é realizado?

46. Existe política de mesa vazia e tela vazia para reduzir o risco de acessos não autorizados ou danos a documentos, mídia e instalações de processamento de informações?

Proteção contra software malicioso e vírus

47. Todos os computadores possuem anti-vírus instalado?

48. A atualização do anti-vírus é automática ou depende de alguma ação do usuário para atualizar?

49. O anti-vírus instalado nas estações de trabalho é algum do tipo corporativo ou é do tipo individual?

50. Todas as mensagens de correio eletrônico, tanto as recebidas quanto às enviadas são verificadas pelo anti-vírus?

51. Usuários recebem algum tipo de treinamento para a utilização correta do anti-vírus?

52. A política da empresa estabelece o direito de recusa de determinados tipos de anexos ou conteúdos contidos nas mensagens de correio eletrônico?

53. A política estabelece que todos os softwares da empresa são homologados e todos os direitos sobre os mesmos são da empresa?

Procedimentos para acesso à internet

54. Existe uma política de acesso à internet? É de conhecimento de todos?

55. Todos os colaboradores têm acesso à internet?

56. Para a utilização da internet é necessário um ID e uma senha?

57. Existe controle de conteúdo que é permitido acessar na internet?

58. Existe monitoramento sobre os acessos dos usuários? Quais são os dados armazenados para a identificação dos acessos?

59. Qual a freqüência que é checada os acessos dos usuários?

60. A política de acesso à internet define medidas administrativas para tratar os acessos indevidos?

61. É definido na política horário para que usuários possam utilizar a internet de maneira particular? Como isso é controlado?

62. É possível identificar através do login e senha de um usuário, de qual estação de trabalho ele realizou determinado acesso?

63. Usuários são treinados para utilizar a internet de maneira segura?

Procedimentos para uso de correio eletrônico

64. Existe uma política para a utilização de correio eletrônico? É de conhecimento de todos?

65. Todos os colaboradores têm acesso ao correio eletrônico?

66. Existe controle de conteúdo das mensagens recebidas e principalmente enviadas? É de conhecimento de todos?

67. Todos os usuários de correio eletrônico podem enviar e receber anexos?

68. A política estabelece se é permitida a utilização do correio eletrônico para fins particulares?

69. Existe algum treinamento sobre como utilizar o correio eletrônico de maneira adequada à política da empresa? Todos os usuários receberam este treinamento?

Gerenciamento, controle da rede, monitoração do uso e acesso aos sistemas

70 . A criação ou liberação de novos acessos é realizada conforme a necessidade de cada usuário?

71 . Todas as solicitações de acesso são formais e liberadas conforme a hierarquia definida na política? Isso é controlado?

72 . Existe revisão periódica dos acessos?

73 . Existe procedimento para quando usuários forem demitidos da empresa?

74 . Contas de usuários em férias ou afastados são bloqueadas nestes períodos?

Identificação e autenticação do usuário, senhas e processo de logon

75 . A identificação do usuário é individual? Existem senhas genéricas?

76 . Os sistemas permitem conexões simultâneas de um usuário?

77 . Existe um número mínimo de caracteres para a criação de senha?

78 . Os sistemas são configurados para não aceitar a criação de uma senha considerada fraca?

79 . Os sistemas são configurados para bloquear o usuário quando houver um determinado número de tentativas de entrada inválidas?

80 . A senha expira após um determinado período, forçando o usuário a trocá-la?

81 . É permitida a repetição de senha?

82 . O login é bloqueado automaticamente se houver um tempo de inatividade grande?

83 . São armazenados os logs de acesso dos usuários, para fins de auditoria?

Backup e Plano de contingência

84 . Existe uma política de backup?

85 . Qual a freqüência da realização de backup?

86 . São realizados testes de integridade nas mídias?

87 . As mídias de backup são armazenadas em prédio ou sala diferente da sala dos servidores?

88 . Existe algum responsável pela tarefa de backup? Como é feito na ausência do responsável? Isso é definido na política e oficializado com todos os envolvidos?

89 . As mídias são identificadas de maneira a ser fácil a identificação das mesmas?

90 . Todos os servidores ou equipamentos considerados críticos possuem backup?

91 . Existe um plano de contingência para a restauração total ou parcial de algum equipamento?

Controle de acesso físico e proteção física as áreas restritas

92 . Existe controle de acesso às salas em que ficam os servidores? Como é feito esse controle?

93 . Existe monitoramento por circuito fechado de TV às áreas de processamento de dados?

94 . A rede elétrica do CPD é estabilizada?

95 . A fiação elétrica que vai para o CPD é independente da que vai para as demais áreas?

96 . Os servidores são ligados em nobreaks? Qual o tempo médio de autonomia?

97 . Existe um plano de manutenção para os nobreaks?

98 . Existe alguma forma de fornecimento de energia alternativo?

99 . Existe sistema de combate a incêndio próximo a sala dos servidores?

100 . Existe sistema de detecção de fumaça no CPD?

101. A sala dos servidores é monitorada por sistema de alarme?

102. O grau de proteção é proporcional aos riscos identificados?

Acesso de terceiros à rede

103. Existe algum procedimento para a instalação de equipamento de terceiros a rede da empresa?

104. Existe controle de entrada de terceiros com equipamentos como notebook e laptop?

Segurança e tratamento de mídias

105 . Existem procedimentos para descarte de mídias (CDs, impressos, disquetes, Hds, etc)? É de conhecimento de todos?

ANEXO A - **Modelo de termo de responsabilidade e Confidencialidade**

Eu, ________________________,declaro, nesta data, ter plena ciência e concordância com todos os termos estabelecidos por este termo de Responsabilidade e Confidencialidade da Organização Ltda. Estou ciente das sanções previamente estabelecidas e divulgadas, sendo que tais determinações deste termo perdurarão inclusive após a rescisão do vínculo de trabalho.

Firmo o compromisso de seguir todas as considerações abaixo:

- Não divulgar quaisquer informações da organização, sem a autorização prévia.
- Manter a confidencialidade das senhas sob minha custódia, seguindo todos os procedimentos e políticas adotados.
- Não utilizar os equipamentos para nenhuma outra finalidade que não seja aquela ligada às atividades da organização.
- Obter aprovação formal para a entrada ou saída de equipamentos e informações.
- Não utilizar softwares que não sejam homologados.
- Utilizar o recurso de correio eletrônico somente para fins profissionais, autorizados à Organização Ltda a leitura de todas as mensagens trafegadas.
- Devolução, em caso de desligamento, de todo e qualquer material de utilização da organização.
- Informar imediatamente qualquer violação das normas estabelecidas, incluindo as violações não intencionais e culposas.

Confirmo que li e entendi a Política de Segurança da Informação e que irei seguir todas as determinações por ela realizadas fielmente.

Local, ___ de ____________ de 20__.

____

Nome e assinatura do Colaborador